S. Hrg. 101-73

VULNERABILITY OF TELECOMMUNICATIONS AND ENERGY RESOURCES TO TERRORISM

HEARINGS

BEFORE THE

COMMITTEE ON
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

ONE HUNDRED FIRST CONGRESS

FIRST SESSION

FEBRUARY 7, 8, 1989

Printed for the use of the Committee on Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 1989

For sale by the Superintendent of Documents, Congressional Sales Office
U.S. Government Printing Office, Washington, DC 20402

S401-35

COMMITTEE ON GOVERNMENTAL AFFAIRS

JOHN GLENN, Ohio, *Chairman*

SAM NUNN, Georgia
CARL LEVIN, Michigan
JIM SASSER, Tennessee
DAVID PRYOR, Arkansas
JEFF BINGAMAN, New Mexico
HERBERT KOHL, Wisconsin
JOSEPH I. LIEBERMAN, Connecticut

WILLIAM V. ROTH, Jr., Delaware
TED STEVENS, Alaska
WILLIAM S. COHEN, Maine
WARREN B. RUDMAN, New Hampshire
JOHN HEINZ, Pennsylvania
PETE WILSON, California

Leonard Weiss, *Staff Director*
Stephen M. Ryan, *Counsel*
Jo Anne Barnhart, *Minority Staff Director*
Michal Sue Prosser, *Chief Clerk*

CONTENTS

Opening statements: Page
- Chairman Glenn 1, 51
- Senator Lieberman 3
- Senator Cohen 4
- Senator Roth 15
- Senator Sasser 54

WITNESSES

Tuesday, February 7, 1989

Charles C. Lane, staff investigator, Committee on Governmental Affairs 6

N. Richard King, executive director, Illinois Commerce Commission, accompanied by Thomas W. Ortciger, director, Illinois Emergency Services and Disaster Agency, and Clyde Kurlander, general counsel, Illinois Commerce Commission 15

Lt. Gen. Lee M. Paschall, USAF (Ret.), former Director, Defense Communications Agency, and John C. McDonald, Chairman, Committee on the Review of Switching, Synchronization and Network Control in National Security Telecommunications, National Research Council, National Academy of Sciences, National Academy of Engineering 22

Thomas A. Norman, vice president of Engineering and Operations, United Telecommunications, Inc., on behalf of the National Security Telecommunications Advisory Committee, and Benham E. Morriss, deputy manager, National Communications System 36

Wednesday, February 8, 1989

Robert K. Mullen, Ph.D., independent consultant 55

Randall W. Hardy, superintendent, Seattle City Light, Seattle, WA 59

Charles H. White, division staff executive, Power Equipment Division, National Electrical Manufacturers Association 64

David B. Hinman, manager, Corporate Security, Alabama Power Co 68

Michehl R. Gent, president, North American Electric Reliability Council 70

Badolato, Edward V., Deputy Assistant Secretary for Energy Emergencies, U.S. Department of Energy 82

Alphabetical List of Witnesses

Badolato, Edward V.:
- Testimony 82
- Prepared statement 296

Gent, Michehl R.:
- Testimony 70
- Prepared statement with an attachment 282

Hardy, Randall W.:
- Testimony 59
- Prepared statement 258

Hinman, David B.: Testimony 68

King, N. Richard:
- Testimony 15
- Prepared statement with attachments 109

Kurlander, Clyde: Testimony 15

Lane, Charles C.:
- Testimony 6
- Prepared statement 93

Page
McDonald, John C.:
    Testimony 22
    Prepared statement 188
Morriss, Benham E.:
    Testimony 36
    Prepared statement 229
Mullen, Robert K.:
    Testimony 55
    Prepared statement with attachments 239
Norman, Thomas A.:
    Testimony 36
    Prepared statement with attachments 207
Orteiger, Thomas W.: Testimony 15
Paschall, Lt. Gen. Lee M.: Testimony 22
White, Charles H.:
    Testimony 64
    Prepared statement with an attachment 266

APPENDIX

Prepared statements of witnesses in order of appearance 93
"Spetsnaz: The Inside Story of the Soviet Special Forces," excerpt, by Viktor Suvorov, defector from GRU (Soviet Military Intelligence) 332
Threat Advisories from the Department of Energy's Office of Energy Emergencies 351
Statement of the American Petroleum Institute 359
"Report of the Interagency Group on Energy Vulnerability: November 1986–November 1988," January 1989, prepared for the Senior Interagency Group for National Emergency Preparedness 363

VULNERABILITY OF TELECOMMUNICATIONS AND ENERGY RESOURCES TO TERRORISM

TUESDAY, FEBRUARY 7, 1989

U.S. Senate,
Committee on Governmental Affairs,
Washington, DC.

The Committee met, pursuant to notice, at 9:37 a.m., in room SD-342, Dirksen Senate Office Building, Hon. John Glenn (Chairman) presiding.

Present: Senators Glenn, Lieberman, Roth, Stevens, and Cohen.

OPENING STATEMENT OF CHAIRMAN GLENN

Chairman **Glenn**. The hearing will be in order.

Today, the Governmental Affairs Committee will begin 2 days of public hearings to review a very sensitive but absolutely vital policy issue, and that is how well the U.S. Government and industry are organized to repel any attacks and to sustain and repair vital services provided by our telecommunications system, by the electrical generation and transmission system, and other bulk energy resources such as oil and natural gas pipelines.

This hearing is not called specifically to pinpoint certain points in our systems that would be particularly vulnerable, and I want to stress that. The hearings will not be a blueprint that could guide anyone interested in conducting terrorist activities. But, there are reminders that we cannot ignore this problem. Today, we will have testimony concerning a fire at a telephone installation in Illinois, which left tens of thousands of persons without telephone service, some for an extended period of time. Do we consider it a national danger that 10,000 people or so were out of telephone service for a while? No, we do not.

Tomorrow, we will hear about a blackout caused by the loss, through fire, of a single electrical installation, which crippled the downtown of Seattle, Washington. Both of these events were accidents and were not the result of sabotage. But these incidents caused widespread hardships for the members of those communities and the issue for these hearings is whether, if you had a better organized effort on a major scale that was not just an accident, the events occurring at the same time could be adequately dealt with by industry and government.

In a world where airplanes with innocent civilians aboard are blasted from the skies in acts of cold-blooded murder, we do not avoid talking publicly about airport security. In like manner, we should examine the robustness and redundancy of our telecommunication and energy networks, and the sufficiency of the government's preparations to assist in reducing existing vulnerabilities gradually over time. In other words, how are we organized, who is responsible, are they on top of what we see as the problem, and are their efforts adequate?

Frankly, there is a great deal of information publicly available which indicates the vulnerability, but less hard analysis, as to what we should do about it and how organized we are to deal with it.

Just some of the background material that was developed for these hearings indicate that we have some 46 different reports to the Congress, hearings, energy vulnerability assessments, books and articles and articles that have occurred mainly since 1982 that take on or describe the vulnerabilities that occur within our system.

As recently as yesterday, The Wall Street Journal had—I do not know whether this just happened to be leaked because the hearing was going to be held today or not, I cannot say that—nevertheless, the title of an article in The Wall Street Journal of yesterday, Monday, says, "Energy Department Reportedly Warns of Terrorist Threat to Energy Facilities," and it details some of the concerns and some of the efforts. One of our witnesses this morning will address this, I am sure, from the Energy Department.

So, this indicates a growing awareness of the problem that we are taking on this morning. Clearly, there is a balance as to what aspects of this problem we wish to discuss publicly and those we wish to discuss privately. No specific detailed locations should or will be given of critical installations during this hearing.

Further, I am also specifically directing this to all our witnesses, they may refuse to discuss publicly any issue which they believe might jeopardize the security we are seeking to foster. In that case, if we feel it is important enough, we will go into executive session.

With that said, we cannot bury our heads in the sand and refuse to address the vulnerabilities or what we can do to reduce them because of an unreasonable fear of raising the topic. Past attacks on energy installations should not bring down a curtain of silence on the subject.

Our country is in a unique situation, because so much of our vital infrastructure is privately owned and operated. These industries are responsive to market conditions. There are some 3,500 electric utilities in this country. Now, how do we deal with all of them and assess the risks posed on each or on the grids into which they feed? Ten years ago, we could have consulted AT&T and been fairly certain that we understood the degree of industry preparation, in the telecommunications area, to a terrorist threat.

Today, each of the seven regional operating companies and their common operating arm, Bellcore, as well as the long distance carriers and non-network service providers, would need to be consulted. At a minimum, we must insure that we understand the changes occurring in the marketplace which either increase or decrease our vulnerability to terrorist attack.

The government structure responsible for responding to this problem is largely ad hoc. There are a number of different entities assigned to different parts of it, and we want to look into that. During the Reagan administration, the National Security Council staff took an active role in policy coordination and oversight regarding the safety of the networks, and that was good. The NSC was positive in its results.

It helped foster a high level of involvement between industry and government by the creation of a Telecommunications Advisory Committee—NSTAC, the National Security Telecommunications Advisory Committee. NSTAC was comprised of the chief executive officers of 30 companies, who met periodically and supplied the drive and commitment of staff time to provide government and industry a forum of shared programs, study committees and recommendations for improvement.

I think one of my first recommendations as a result of our own study is that NSTAC, or something very much like it, should continue in the new administration. In fact, all currently operating forms of industry and government cooperation should be nurtured, not stopped.

All of these government preparations are primarily aimed at continuing essential government services, but not necessarily the services utilized by members of the public. It is protecting the public, in a more generalized sense, upon which we are focused.

I am hopeful that these hearings will provide us with a number of recommendations for practical advancement of government activity, and for renewed emphasis on industry and government cooperation.

Before I introduce our witnesses today, Senator Lieberman, do you have any comments to make?

OPENING STATEMENT OF SENATOR LIEBERMAN

Senator **Lieberman**. Thank you, Mr. Chairman, and good morning.

Today, this Committee examines a subject of paramount importance, which is the vulnerability of our Nation's telecommunications system and bulk energy systems to terrorist attack. Obviously, this is an unsettling and an uncomfortable topic, but the threat is real and the stakes are enormous, and so with the very wise limitations that you have applied that relate to national security, we must discuss it.

In fact, Mr. Chairman, may I say that my service in the Senate and on this Committee is still young enough that I can congratulate the Committee without seeming to congratulate myself. I therefore want to tell you, as I arrive here as a new member, how impressed I am by the Committee's decision to undertake this assignment and by the work that the staff has done.

It seems to me that this is a particularly pressing time for the United States to be considering the vulnerability of our civilian infrastructure to terrorist attack, because we seem to be entering a new era in our foreign relations, an era in which our concept of defending the national security may be redefined or at least expanded. It may be that the most serious threats to our security, we will conclude, will come not from Soviet nuclear attack but from terrorist assaults by smaller renegade nations and outlaw groups.

While we have not suffered from direct terrorist attacks here, clearly some attempts have been made. Just last week, I noticed that the U.S. Attorney's office in New Jersey alleged that a suspected Japanese Red Army terrorist, who was arrested last April, was working with Libya to detonate bombs at three different locations in Manhattan.

We as a nation have always had the ability to pull together and react effectively in times of crisis. We have too often been less effective at planning and prevention, and that is why I think these hearings are so important today.

Now is the time to increase our vigilance against the possibility of future terrorist attacks. While our military installations may be relatively secure, as your statement indicates, Mr. Chairman, our civilian infrastructure may well not be.

Telecommunications and energy systems are attractive targets for terrorists and may, if we do not act, prove to be our national achilles Heel. Virtually every aspect of American society today depends on the uninterrupted flow of electricity, natural gas and petroleum and on telephone and data transmission services. Our energy and telecommunications systems are not only vast, but as I am sure we will hear today and tomorrow, are difficult to protect and are also dependent on one another.

Even the introduction of new technologies, such as fiber optics, creates problems. Fiber optics vastly improved our telecommunications system—a single hairthin fiber of glass can carry 8,000 conversations simultaneously—but it may also have enhanced the ability of a terrorist to disrupt telephone service to a large region.

This is an area where private enterprise dominates but, as you suggested in your statement, Mr. Chairman, it is also clearly an area where public and private sectors must cooperate for the national good.

State and local governments I think may have a constructive role to play here. In the wake of Hurricane Gloria a few years ago, when thousands of residents in our State were left without telephone or electric service for several days, the Connecticut Legislature enacted a law requiring each utility to prepare plans for restoring post-emergency service and to file those with State agencies and with every municipality located in the utility's service area.

To my knowledge, there is currently no central Federal repository for that kind of State information and no one Federal agency responsible for coordinating the protection and restoration of energy and telecommunications networks.

Mr. Chairman, as uncomfortable as these issues may be, we cannot ignore them in the hope that disaster will not strike. These hearings are an important step toward reducing our vulnerability to terrorism and preventing a disaster from ever occurring.

Thank you very much.

Chairman GLENN. Thank you.

I missed Senator Cohen's entry here. I should have called on him first this morning.

Mr. Cohen?

OPENING STATEMENT OF SENATOR COHEN

Senator COHEN. Mr. Chairman, I would join in commending you for holding this hearing and point out that this is not the first set of hearings that have been held by this committee. As I recall, we held hearings back in 1981 or 1982 dealing with the very same subject matter. So the problem is not that we have said so little, but we said so much and done so little to deal with the problem.

My colleague from Connecticut is quite right in pointing out that the United States has been relatively free from terrorist actions. That is a result of two things: Number one, we have been lucky; and, number two, we have been good.

The FBI has done a tremendous job in preventing a number of planned terrorist actions in this country, and we should keep that in mind as we debate budget deficits in terms of what it is going to require in the future to deal with this.

I would say, Mr. Chairman, that we are spending billions of dollars to defend ourselves, but it is very easy to see that we can be undone by a dozen hands and a few thousand dollars, and so it is important, even though we have talked about this issue before, to constantly reaffirm the need to take the kind of protective measures that are necessary.

We spend billions of dollars, for example, on constructing ships in the State of Connecticut, Maine, and elsewhere; and yet a few years ago we found that a group of nuns were able to sail up a river in a canoe and go to the Electric Boat Yard and damage one of our nuclear subs, because the coastline was relatively unprotected and there was little boat yard security.

Well, we have taken certain measures since that time, primarily as a result of a ventilation of these issues. So, I think it is important, Mr. Chairman, that you constantly reiterate the need to deal with this before it happens, not after.

Chairman GLENN. Thank you.

Senator Stevens?

Senator STEVENS. I have no statement.

Chairman GLENN. Thank you.

We have two different groups that will testify today. We have first today Mr. Charles Lane. He has been a staff investigator for the Committee on Governmental Affairs. Following him will be Mr. Richard King, Executive Director of the Illinois Commerce Commission, accompanied by Mr. Thomas Ortciger, Director of the Illinois Emergency Services and Disaster Agency.

We have two panels: Panel 1, Mr. John McDonald, who is chairman of the Committee on the Review of Switching, Synchronization and Network Control in National Security Telecommunications of the National Research Council, National Academy of Sciences and National Academy of Engineering; Lt. Gen. Lee M. Paschall, USAF (Retired), Director, Defense Communications Agency; and panel 2, Mr. Thomas A. Norman, Vice President of Engineering and Operations of United Telecommunications, representing the National Security Telecommunications Advisory Committee; and then Mr. Benham E. Morriss, Deputy Manager, National Communications System.

I want to give a lot of credit this morning to our first witness, Chuck Lane, Charles Lane. We have this interdepartmental fellowship program, an exchange program within government, where people from one department come for a year to study and get a little experience in some of the other branches of government.

The Secret Service is one of the participants in that program, and Chuck came to us just about a year ago on loan to this Committee. He performed the field work on this investigation for the Committee and did an outstanding job on it. It is a very big, thick report that I have read in its entirety. It is over a hundred pages. He has done a superb job of getting all this information together over the past year. The work that he did is really the bulk of the work that went into the preparation for these hearings, so I want to thank him publicly this morning.

He will be leaving the Committee within a couple of weeks and going back to his duties in the Secret Service. We wish him well. The Secret Service's gain is our loss, as far as the work goes that he has done this past year.

Chuck, we thank you very much for it and the effort that you have put into this thing, along with the dedication that you have displayed. It has not been just a daytime job with Chuck. He has lived this project over the past year. So, we thank you very much for that and look forward to your testimony. Proceed.

TESTIMONY OF CHARLES C. LANE, STAFF INVESTIGATOR, COMMITTEE ON GOVERNMENTAL AFFAIRS [1]

Mr. LANE. Thank you, Mr. Chairman and members of the Committee.

I have been with the Secret Service for 17 years. That career has included assignments in intelligence, in security and in investigations. In February of 1988, however, I was detailed to the Committee on Governmental Affairs. All of the activity in which I have been involved since that date has been exclusively associated with the Committee, and is in no way affiliated with either the mission, nor the organization of the U.S. Secret Service.

Shortly after my arrival on the Committee, we initiated a fact-finding investigation to determine whether the energy distribution and telecommunications networks were unnecessarily vulnerable to man-made disruptions, and if so, to identify Federal and private initiatives designed to mitigate those vulnerabilities.

The investigation attempted to identify: One, the level of the threat, two, the actual vulnerabilities within the networks, three, the consequences of their exploitation, and four, the organizations within the Federal Government and private sector which were most directly affected by these issues.

The primary objective of the investigation was to determine whether a terrorist group—perhaps numbering 6 to 12, to 20, using conventional weapons such as plastique explosives, incendiary devices, backhoes, or even software, could significantly disrupt the Nation's energy distribution or telecommunications networks in a peacetime environment.

Much of the information gathered by the Committee was obtained from unclassified sources and other open source material. It was supplemented with information obtained from more than 100 interviews conducted with policymakers, managers, analysts, and technical experts, in both the private and public sector.

---

[1] See p. 93 for Mr. Lane's prepared statement.

Although we recognize that this is a sensitive subject, in the United States the vulnerabilities of our infrastructures have been frequently exposed. If I can direct your attention to the posters to your left, it becomes obvious that the issues which we are about to discuss have already been identified in the media.

These are excerpts from press articles which appeared in major media forums during the period of the Committee's review. The first article discusses an April incident involving the arrest of a Japanese Red Army suspected terrorist, and suggests that the whole Northeast could be blacked out by a handful of terrorists.

The second article describes the serious impact of raids on the electrical grid in El Salvador in May. The third article presents observations following the fire at the Hinsdale, Illinois, telephone switching station, and suggests that significant vulnerabilities exist in the phone system. November produced a fiber-optic cable break, and the fourth article suggests that fiber-optic cable has introduced a new vulnerability concern.

Next, we have advertising promoting a 2-night examination of utility vulnerability on an evening news show. In the same month, an article appeared describing the vulnerability of the Strategic Petroleum Reserve to terrorist attacks.

These articles and others like them have attempted to provide accurate representations of a very complex subject of vulnerability. The public is being told that vulnerabilities exist. Well researched and revealing articles have been and will continue to be published.

Our examination examined the distribution networks for crude oil and petroleum products, for natural gas, for electric power, and for telecommunications.

The networks reviewed are almost exclusively municipally, cooperatively, or investor owned. The resources to operate, evaluate, and reconstitute the networks are held by the companies. As economic enterprises, there are legitimate proprietary concerns which factor heavily into the decisions made by these companies as to what represents adequate investments in security and reliability measures.

The communications and energy systems were selected because they are vitally important to the public welfare, the national economy, and the national defense, but the Federal Government owns or operates a relatively insignificant portion of either. In a peacetime environment, the Federal Government has almost no oversight authority relating to the protection of the networks.

In 1988, Oliver Revelle, Executive Assistant Director for the FBI, told a Senate subcommittee that "it is unrealistic to assume that we have the ability or resources to guarantee protection to our Nation's infrastructure industries from every conceivable terrorist attack."

If networks and infrastructures cannot be physically protected, then the capability to detect imminent assaults before they occur becomes increasingly important. Fortunately, the FBI can claim a number of successes in combatting terrorism.

In spite of these successes, however, the continuing but unsuccessful attempts by the United States to close its borders to both drug traffic and illegal aliens has demonstrated how easily people and weapons can be smuggled into the country and potential terrorist support networks are in place in the United States.

Even U.S. street gangs could provide the necessary support. Several are known or suspected of having hostile foreign connections. For instance, Los Angeles street gangs have been accused of involvement with the Medellin Cartel, and members of the El Rukn gang of Chicago have been convicted of conspiring with the Libyan government.

Because the United States has a tradition of involvement in the global political arena, the possibility always exists that some group or individual will seek revenge or policy influence through the commission of acts of terrorism. Traditionally, the concern for such acts has been associated with international terrorists, and these groups continue to pose a potential threat.

Significant international terrorist groups, on the other hand, have never targeted the infrastructures of the United States, according to the analysts that I have interviewed. If such targeting occurred now, some speculate that it would more than likely result from encouragement by a hostile foreign government, such as Libya or Iran.

A domestic terrorist organization, on the other hand, may present an equally significant threat. Such groups are generally made up of individuals whose ideologies encourage them to defy Federal authority. Members can usually move freely about the country and are comfortable operating within its boundaries.

Historically, terrorists have selected high-profile targets for their symbolic value, and with the intent to kill, or to bargain with human life. This has resulted in the selection of airliners, military facilities, diplomatic facilities, and other frequently selected targets.

The potential threat, however, cannot be dismissed, for if targets are selected for their true value, either to cripple a nation's economy, or as an act of defiance or revenge, these networks present tempting targets. The networks are exposed, they are vulnerable, chances of a successful attack are highly probable, and significant economic damage can be inflicted as a result.

For these reasons, it is apparent that a serious effort must be made to understand what impact terrorist attacks can have on the networks, to identify and initiate measures to "harden" networks to withstand assaults, and to make plans to recover services lost as a result of successful attacks. This conclusion is based on the simple recognition that the threat level changes much more rapidly than the vulnerability level. The tragic destruction of the Pan Am airliner in December 1988 provided brutal notice to that fact.

By their physical nature, networks provide an inexhaustible number of potential targets. Physically protecting a network against any and all possible disruptions is economically impossible.

Given the inherent vulnerability in these networks, the question as to whether they are unnecessarily susceptible to extended disruption by a sabotage or terrorist can only be answered by determining: One, what critical nodes or choke points exist, two, whether they have been afforded appropriate attention, and three, whether system redundancies and recovery planning exists in the event of a successful attack.

Opinions differ as to whether the Federal Government has a need or right to know where specific critical nodes exist within a network. The electric power industry feels strongly that it does not. The Department of Energy has currently taken the position that there is no need to establish a national list of critical nodes which would be held by one or more Federal agencies. The Department of Defense, on the other hand, feels that it is necessary to identify and establish a list of critical nodes vital to defense related industries and installations within each Army district of the United States.

Systems are constructed differently, and critical nodes vary. Generically speaking, a critical node could include a pump station on a liquid pipeline, it could include a compressor on a natural gas pipeline, it might be an extra-high voltage transformer and substation in the electric transmission network, switching centers in the telecommunications networks, control centers or portions of transmission or distribution routes.

In most cases, the reconstruction of a critical node involves the replacement of expensive, custom-designed, long lead-time components which require a significant and a currently deteriorating manufacturing base.

Critical nodes are rarely afforded any more protection than any other node in the system, and in some instances the loss of one or a multiple of similar nodes may create a situation in which the populace of a city, State, or a larger geographic region could be generally denied the service or product provided by the system for days, weeks, or longer. Fortunately, our systems are robust—without real expertise in choosing targets, the impact of even a serious attack may not be catastrophic in a national security sense, but the results could have a profound effect on the community.

Although our investigation focused primarily on long-distance distribution systems, any major metropolitan area has the same problem. Most have a relatively small number of critical nodes supporting a service such as phone, electric power, or petroleum and gas supply. Though it may be of limited duration, a major portion of any metropolitan area will be denied a service by eliminating those nodes. In some scenarios, a portion of the disruption might continue for several days, weeks or months.

To heighten our concerns, there are several standard operating practices observed in industry which increase vulnerability concerns. I would not attempt to list them all, but let me give you some examples.

It is common practice to place spare units next to operating units. Examples would include items such as pipeline pumps and spare extra-high voltage transformers.

It is not unusual for major pipelines to be operated from a single control center, with no alternate control center available.

It is becoming common practice now to concentrate high-volume switches in a single structure, three to four switches are common.

It is also common to install essential, expensive equipment in a facility that is generally protected by little more than a fence. Sometimes these items are not even enclosed inside the structure.

Does poor physical security contribute to vulnerability concerns? That question is difficult to answer. In some cases, increased physical security measures appear to be a simple solution to the problem of exposed facilities. In other cases, it may be the least productive and most expensive approach to ensuring that the service is maintained.

In 1979, the Government Accounting Office issued a report entitled "Key Crude Oil and Product Pipelines are Vulnerable to Disruptions." That report documented instances of unlocked doors and gates at key facilities, loose or non-existent key and pass control systems, generally poor physical security plans associated with a number of key pipelines. Many of those conditions still exist. Two operators of major pipelines responded to the 1979 GAO report, asserting that even a highly sophisticated physical security program would not succeed in eliminating the vulnerabilities. Other industries share this opinion.

Ironically, both the Government and the industry, responding to other legitimate policy concerns and operational necessities, have made the job easier for a potential adversary. For instance, the 100th Congress passed legislation which, in the interest of public safety, requires pipeline operators to provide detailed maps of their systems to State and local governments, to allow for emergency planning and public safety education.

Environmental impact studies, as well as reports accumulated by DOE, FERC, FCC, and Transportation often contained detailed information and are available to the public. Relatively detailed maps of the various pipeline systems and the electrical power grids can also be purchased from the industries themselves. An example of that is displayed again to your left. This is a typical map representing pipeline routes across the Nation, and behind that is a similar display for the major electric transmission grids, complete with identification of substations and so forth.

It is undesirable and impossible to reverse these policies. However, such policies do increase vulnerabilities by making information available.

Coincidentally, a GAO report released in December 1988, documented the use of material obtained from a library by a mock "terrorist" team during an assault on the Strategic Petroleum Reserve in 1987.

Accidents and natural disasters have provided more than an adequate indication of the potential consequences of mass disruptions of crucial systems. Several incidents have occurred in recent years that demonstrated the reliance of the American public on these networks and the potential catastrophe associated with their destruction.

The first to come to mind are the massive electrical outages which occurred in New England in 1965 and again in New York in 1977, but less spectacular events have occurred in the months in which this committee conducted our review.

A major refinery in Louisiana exploded and burned in May of 1988. Press reports at the time estimated the loss at $100 million. Also in May, we had the Hinsdale switching station fire, followed by a fire in an electrical vault in Seattle in September, which put a 50 square block of the city in darkness for several days. November produced the fiber-optic cable break on a line that generally carried 200,000 calls per hour.

In isolated cases, help and expertise can be brought in from unaffected areas. However, if terrorists were to target such systems and achieve significant destruction at multiple sites, the impact of such disruptions could have a dramatic and catastrophic impact on the public welfare, and on the local, the regional, and perhaps national economy.

For instance, a loss of a major petroleum pipeline could send gasoline prices skyrocketing, require localized rationing, and require a herculean effort to find alternative transports for supplies. The loss of electric power in a major area has already been demonstrated, and if a natural gas pipeline is lost, there is simply no other mode of transportation available. Under the worst conditions, an extended disruption could even interrupt service and require pilot lights to be relighted.

The Federal Government has a responsibility of maintaining a defense capability and protecting the welfare of the public. Since the energy and telecommunications networks are vital to that effort, the Federal Government must be able to effectively work through private industry to achieve those objectives. But opinions differ as to what constitutes an adequate commitment of resources and acceptable level of risks. In many ways, the vital question of who is going to pay to mitigate the risk dictates the ambiguity of responses.

The approaches used by the Federal Government in addressing energy and telecommunications concerns vary in several significant respects. The National Communications System [NCS], with almost 100 employees and an annual budget of approximately $75 million, works closely with a committee appointed by the President called the National Security Telecommunications Advisory Committee [NSTAC]. This committee consists of executives representing the top 30 telecommunications providers in the Nation.

Under the committee's direction, industry task forces continually identify and research potential problems, and work with the NCS to correct them. In addition, it is the intention of the Federal Government to supplement the physical assets of the public switched network.

Energy issues are addressed by the Office of Energy Emergencies, with 71 employees and an annual budget of $6.2 million. The energy effort is not assisted by anything equivalent to NSTAC. The Department of Energy attempts to reduce vulnerabilities through outreach programs, involving studies, awareness programs, and exercises involving simulated disruptions.

In summary, this investigation concluded that the networks of the United States are vulnerable to multisite terrorist attacks, that is, that targets are likely to be destroyed. However, the redundancy built into the networks make them very dependable, and the real question is what level of service would be lost from such an attack. In many cases, the consequences appear to be manageable. In a few cases, perhaps too many cases, the consequences are potentially catastrophic.

Beyond the more clearly drawn NSEP responsibilities of Federal Government agencies, there is a vacuum in the current authority, planning, and ability to impose requirements to ensure a service capability to the public. Most authorities and responsibilities are addressed only to NSEP, National Security Emergency Preparedness, considerations. While NSEP programs provide some measure of protection to the public in nondeclared emergencies, there are no programs designed specifically to ensure the public a minimal level of service, and there can be serious consequences when that service capability is lost, as we will hear next regarding the Hinsdale fire.

Mr. Chairman, there are some very complicated issues to be explored regarding vulnerabilities and the reliability of service. I hope this overview assists the Committee in its review.

Thank you.

Chairman GLENN. Thank you very much, Chuck. You have performed yeoman service this year, as I pointed out before your comments. I will keep my questions and my comments very short.

Our problem, as you define it, is what percent of an energy system or a communications system could be knocked out, for what period, and in what areas of the United States.

We have referred to just a couple of things, the Illinois situation that happened on a small scale and others that you mentioned. But, I think, from looking at this thing from your study, the others who looked at it feel, that very few people, properly positioned, could do a tremendous amount of damage to big chunks of this country for quite a lengthy period of time.

Our next problem then, as you say, is that we want to define who is going to look into this, follow it and see what can be done to reduce this kind of vulnerability. We have a number of witnesses here this morning and we want to get on to it, but I would just ask one question.

Who has the overall responsibility in this area now?

Mr. LANE. The National Security Council has policy responsibility for the U.S. Government with regard to NSEP considerations, and then those individual responsibilities are subdelegated to the appropriate agencies within the Federal Government. The Department of Energy addresses energy issues and the National Communications System addresses the telecommunications issues on behalf of the Federal Government. The FBI has also been tasked to assist under the most recent executive order.

Chairman GLENN. As I indicated in my opening remarks, we had some 46 different studies and groups who have looked at this thing over the past several years. It seemed, in our eyes, that there needed to be a more clearly defined cooperative effort. Not defining—once again, I would say not defining specific spots, but, as you said, choke points where certain supplies come down and where damage to a very few spots could really knock out that particular supply to large parts of the United States. That is what we want to define: What organizations are taking on that responsibility to monitor these things and determine what can be done about them?

Senator Cohen?

Senator COHEN. Mr. Chairman, thank you.

Just very briefly, Mr. Lane, you said that without real expertise, the impact of such attacks may not be critical. The corollary is that with real expertise, it would be critical.

Mr. LANE. I think with real expertise or, with a little luck, it can be critical.

Senator **Cohen**. Also, in your statement, I think you referred mostly to either domestic terrorists groups as such or a third-world nation. You did not refer to SPETSNAZ, the potential for Soviet special force operations, in this country. I do not know if you had a chance to read Victor Sovorov's book, called "The Inside Story of the Soviet Special Forces," but it has some interesting reading in the final chapter. I am not sure what the copyright restrictions are, Mr. Chairman, but I recommend you include that final chapter in our proceedings.[1]

Chairman **Glenn**. We will check on that and include it in our record. I believe we are exempt from copyright, so long as it is part of the Committee record. We will check that. The Committee is not going to put out taxpayers' money for royalties, I do not believe.

Mr. **Lane**. Senator, if I could respond to that, we are aware of the concern with the capabilities of special operations groups and we did touch on that in our investigation. But for the purposes of this hearing, we wanted to restrict our focus on a terrorist incident, because we recognized that a special operations group would have far more capabilities in terms of manpower, resources, intelligence, and so forth, and would be considerably more effective than the average terrorist.

Senator **Cohen**. In fact, it may take fewer in the way of manpower, if they are really expert, if you have fewer people with fewer systems, with more concentrated impact.

Mr. **Lane**. Absolutely.

Senator **Cohen**. Thank you.

Chairman **Glenn**. Thank you.

Senator Lieberman?

Senator **Lieberman**. Thank you, Mr. Chairman.

Mr. Lane, again thank you for your extraordinary work and service here. Two questions, briefly. Running through the discussions of this problem, particularly from people in the private sector in telecommunications and energy, is the conclusion that it is ultimately impossible to protect these systems. The best that we can do is to build in "redundancy"—a technical term that I understand to mean a fall-back position, the ability to recover from an attack. Do you accept that conclusion, or do you think there is substantially more we can do to protect these systems from terrorist attack?

Mr. **Lane**. Senator, I really am not qualified to respond to that question. There are so many considerations involved in the operation and technical construction of each these systems. Quite frankly, I do not have the expertise to know whether it is practical to add certain physical protection features at critical substations, for instance. It is not as simple as constructing a large fence around the compound and putting in an intrusion detection system, because many of these stations are located hundreds, maybe thousands of miles from the central facility, and there is no way that there can be a response capability to them.

I think it is fair to say that physical security in itself, whether you are talking about engineering design, intrusion devices, alarms, whatever, address risk reduction, that is, they cut down on the opportunities, but they cannot be relied upon to eliminate them. So, depending on the perseverance, or personal commitment of the adversary, it is hard to say whether they would be effective. Beyond that, I could not answer your question.

---

[1] See p. 332.

Senator LIEBERMAN. You do not reach the conclusion, based on your investigation of whether we ought to be doing more to protect the systems, as opposed to doing more to be ready to recover from an attack?

Mr. LANE. My conclusion—and I think this is consistent with conclusions that you would hear endorsed by specifically the Department of Energy, because that is where most of my concern is—is that there are some areas that need some immediate attention, and they are aware of them and I think, yes, there is more that could be done than is being done currently.

Senator LIEBERMAN. The second question: In your statement, you mention that the Department of Energy has taken the position that it is not necessary for the Federal Government to maintain, in some agency, a list of what you call the critical nodes in each of these basic industries. The Department of Defense has apparently taken the opposite position, and I gather that the electric power industry has said that it does not want to maintain a list of critical nodes.

Does this disagreement suggest to you, based on your in-vestigation, that there is need for a central coordinating Federal agency to make these judgments? Do you support having a Federal agency maintain a central list of these critical nodes?

Mr. LANE. Senator, I really again would like to stay out of offering my opinions as to what is the best way to approach it. Certainly, the Federal Government does not have the capability to protect all of the critical nodes within these systems, so from the Department of Energy's standpoint, there is some justification, I would think, for not creating a critical list.

If you have a list of critical nodes and you cannot do anything with it, you have to ask why you need to have it. Certainly the industries need to know where their critical nodes are in order that they can take appropriate measures to protect them.

The case with the Department of the Defense is a little different. The Department of Defense, in a scenario in which it would protect critical nodes, is looking at a case in which we are going into a surge condition for some sort of military buildup—where there is a reason to be concerned with the protection of those facilities at the national level. Therefore they do need, I believe, to have a knowledge of where they are, so that they can immediately get resources to them.

Senator LIEBERMAN. Thank you, Mr. Chairman.

Chairman GLENN. Thank you.

Senator Roth just arrived, and we are about to move on to our next witness. Do you wish to ask any questions?

Senator ROTH. No. I would ask that my opening statement be inserted in the record.

Chairman GLENN. Without objection, that will be included.

[The statement of Senator Roth follows:]

OPENING STATEMENT OF SENATOR ROTH

At the outset, Mr. Chairman, let me say that I wholeheartedly endorse your comments about the need for discretion and good judgment as we approach this issue of the vulnerability of telecommunications and energy resources to terrorism. The threat of disruptions to these major networks is real, but I feel very strongly about our responsibility to conduct these hearings with caution and sensitivity to the potential damage that public discussion of specific vulnerabilities could produce.

We have witnessed far too many tragic incidents in which the loss of American lives abroad has been attributed to terrorist activity to ignore the potential menace of terrorism within our boundaries. Highly-developed technological networks are increasingly being recognized by terrorist factions as promising targets as evidenced by significant attacks on telecommunications and energy systems in El Salvador, West Germany, and Japan. We can ill afford to become complacent merely because we have thus far been able to avoid catastrophic incidents. By the same token, Mr. Chairman, hysteria over our vulnerabilities would be unfounded.

I believe it is very important to bear in mind that we do have mechanisms in place to detect as well as to respond to emergencies of this nature. Our intelligence community collects data continuously and uses that information for preemptive actions. We will hear this morning from the Deputy Manager of the National Communications System and tomorrow from the Deputy Assistant Secretary for Energy Emergencies at the Department of Energy about a large number of ongoing activities the federal government is coordinating to prevent or to respond major disruptions of telecommunications and energy delivery systems.

I agree with you, Mr. Chairman, that coordination and cooperation between government and industry officials are absolutely essential to attaining our goals of reducing vulnerabilities and strengthening security measures. Our intention during these hearings, as I understand it, is to promote continued cooperative efforts and to assure that adequate management systems are in place within the government to further the development of national emergency preparedness planning. Based on a preliminary review of the testimony to be presented, I am confident that we will learn a great deal from our witnesses, and I join you in welcoming them.

Chairman GLENN. Thank you very much, Mr. Lane. We appreciate your efforts in this regard. We may have questions later on.

The next witness is Mr. Richard King, Executive Director of the Illinois Commerce Commission, accompanied by Mr. Thomas W. Ortciger, Director of the Illinois Emergency Services and Disaster Agency.

Mr. King, Mr. Ortciger, we are glad to have you with us this morning. We appreciate you coming in.

Mr. King, if you will proceed.

TESTIMONY OF N. RICHARD KING, EXECUTIVE DIRECTOR, ILLINOIS COMMERCE COMMISSION,[1] ACCOMPANIED BY THOMAS W. ORTCIGER, DIRECTOR, ILLINOIS EMERGENCY SERVICES AND DISASTER AGENCY, AND CLYDE KURLANDER, GENERAL COUNSEL, ILLINOIS COMMERCE COMMISSION

Mr. KING. We have some visuals that we would like to provide for you which may offer some assistance.[2]

Chairman GLENN. Fine, if you would introduce them so we would have their names for the record, please.

Mr. KING. My name is N. Richard King. I am the Executive Director of the Illinois Commerce Commission, and with us today we have Mr. Tom Ortciger, who is the Director of ESDA, and we have Clyde Kurlander, who is General Counsel of the Illinois Commerce Commission.

---

[1] See p. 109 for Mr. King's prepared statement.

[2] The visual information referred to follows Mr. King's prepared statement.

This is just to give you some idea of the geographical area affected by the Hinsdale fire. [Displaying chart]

Good morning, Mr. Chairman and members of the Committee. My name is N. Richard King. The Governor has asked me to thank you for inviting him to appear here today before you. The Governor shares the concerns of this committee. The impact and consequences of the Hinsdale fire are of great personal interest to the Governor. It was Governor Thompson's declaration of the area affected by the fire as a disaster area which initiated the process ultimately resulting in the availability of Federal funds and SBA loans to those affected.

At the Governor's request, Illinois Bell provided $500,000 in grants to 12 communities and fire districts for community and economic development.

The fire, which occurred May 8, 1988, at the Hinsdale Central Office of the Illinois Bell Telephone Company, is now regarded as the most serious fire ever encountered by the telephone industry. The Hinsdale fire disrupted not only local exchange service to approximately 38,000 customers, it also prevented interoffice calls involving more than 40 central offices.

Customers in the regions served by these 40 central offices were also denied access to the long-distance network. In all, there were more than half a million residential and business customers affected by the fire. These customers either made or received about 3.5 million phone calls per day. The geographic extent of the communities affected by the fire are displayed by that visual, and it is also an attachment to the written testimony which I provided to the Committee.

The outage affected all customer groups. Calls for emergency services, such as to the fire or police departments, could not be completed. The Air Traffic Control Center at Aurora lost a large number of voice and data circuits which connected it to O'Hare and Midway Airports. This caused extensive flight cancellations and delays. Hospitals lost the ability to communicate not only with the outside world, but also with various internal entities such as nurses stations, emergency rooms, and operating rooms. Corporations could not communicate with their headquarters or branch offices. Retailers could not verify credit cards. Drug stores could not fill prescriptions.

A major manufacturer of consumer and industrial products whose telecommunications services for its Chicago area facilities was operated out of their office, in Oak Brook, Illinois. All of the company's locations are in constant contact with the corporate headquarters in New York and various other locations nationwide. Fifteen of their company's locations were completely out of service and could not communicate with each other, nor with the rest of their locations throughout the country or overseas.

The Hinsdale Central Office fire caused a total outage to a manufacturer of farm and construction equipment, whose operations are international in scope. The Veterans' Administration initially reported the loss of 23 circuits. These dedicated lines primarily connected the Veterans' Administration's medical centers and regional offices.

The Federal agencies reporting disruptions to their service were the Veterans' Administration, the FAA, the Department of Commerce, the Nuclear Regulatory Commission, and the Department of Energy.

Illinois Bell began the restoration of service with the rerouting of interoffice traffic around Hinsdale on available copper, working copper circuits and with temporary installations of microwave link between the Hinsdale Switching Center and La Grance Switching Center. Service for police, fire department and hospitals was given first priority for the restoration.

Special assistance to residential and business customers served from the Hinsdale Central Office included the following: Setting up three special centers, with a total of 200 lines in the Hinsdale area to provide interim service to business customers, providing free shuttle bus transportation to one of the centers, installing 120 coin phones at 16 special coin trailer locations throughout the affected area, establishing an emergency relay plan to delivery emergency messages to customers in the affected area, making available 200 lines in Chicago for use by business customers.

Restoration proceeded simultaneously on three fronts, on an emergency basis: Equipment to provide local service was procured, installed, and tested; other equipment was obtained and installed to allow resumption of network communications to and from the suburbs and to provide access to long-distance networks. Existing local switching equipment was brought back into service on a temporary basis, restoration of the 36,774 special service circuits was carried out simultaneously with network restoration, but presented special problems.

Restoring these circuits involved locating records containing facility and equipment specifications, re-engineering each circuit and testing it for the correct operational characteristics. The switching equipment, which provided local service for the Hinsdale area, was intact but subject to acid corrosion and unreliable after the fire. Thus, Illinois Bell determined that the local equipment, a 1AESF switch, could not be salvaged and again the process of replacing it.

Between May 11th and May 20th, service was restored in increments. Virtually all 38,000 customers had service by May 20th.

The reason such a fire could have such wide-ranging effects is touched upon in your letter of January 24, 1989, in which you say, "High-volume switching centers are now becoming common place within the telecommunications industry." I discuss in greater detail in my written testimony the development of the Illinois Bell Telephone Network into its current hub configuration, which is this card here [illustrating].

Suffice it to say here that the advent of the fiber-optic technology has made it possible to exceed the capability of existing copper network to carry both voice and data, the greater capability of the fiber-optic technology has allowed the network to be reconstructed into a more economic and efficient pattern.

In the old copper grid network, individual switching centers were connected directly to each other. In the new fiber-optic network, individual switching centers are connected to each other through a central hub. These hub centers function much like large airports, such as O'Hare. Smaller feeder airports route passengers through large airports and then on to other destinations. Similarly, traffic in the smaller surrounding switching centers passes through the hub in order to connect the smaller centers with one.

While the new fiber-optic hub network offers numerous service and economic advantages over the old copper network, the loss of one of these switching hubs such as Hinsdale causes major emergencies and not mere inconveniences.

It is the design of the hub network which renders the system vulnerable to the wide-ranging consequences which I have described to you. While several State agencies with direct responsibilities for telecommunications, fire protection and emergency services worked cooperatively in overseeing service restoration efforts, there is no denying that the potential for devastating consequences existed.

Within 72 hours of the Hinsdale fire, the staff of the Commission decided that the magnitude of the event required a more comprehensive and intensive investigation than had previoulsy been taken anywhere in the country. This added effort was needed to insure the Commission's public service public service mandate was honored.

I believe the multidisciplined and comprehensive approach which, although time-consuming and thus frustrating to me, will yield a final report that will have a high level of credibility for the telecommunications consumers. In a moment, we will have a chart up here which diagrams the organization we put together to monitor the restoration of service and also to monitor the report that the group did for us.

The State of Illinois, through the Illinois Commerce Commission, secured an agreement from Illinois Bell to fund the services of an independent engineering consultant firm to serve at the exclusive direction of the Commission.

Chairman GLENN. Could I ask a question here for just a moment?

Mr. KING. Yes, sir.

Chairman GLENN. I do not want to interrupt you for long. Was this put together only afterwards? This was not in effect before the Hinsdale fire?

Mr. KING. No, sir, it was not before.

Chairman GLENN. This was as a result of it?

Mr. KING. Yes, sir.

The Commission retained the services of Forensic Technologies International Corporation, of Annapolis, Maryland, a nationally recognized consulting engineering firm specializing in fire and failure analysis, to conduct a comprehensive and in-depth investigation into the cause and origin of the fire and to make specific loss prevention recommendations.

On September 6, 1988, an interim summary report on the status of the investigation was submitted by the Office of the State Fire Marshal and the staff of the Illinois Commerce Commission. That interim summary report contained a projection that the final report would be completed by mid-November. However, subsequent evaluations of the schedule and testing requirements rendered that date overly optimistic. The final report detailing the results of the investigation is now due February 28th. Upon its completion, we will make a copy of that report available to this Committee and we stand ready to appear before you again to answer any questions you might have.

Soon after the fire, the Attorney General of the State of Illinois, Neil F. Hartigan, requested the Illinois Commerce Commission to institute a public on-the-record investigation of the fire. The Commission did so. The purposes of that investigation are to inquire into the adequacy of Illinois Bell's provision of telecommunications services, to consider adopting emergency plans for catastrophic incidents, including emergency alternative services, and to assess the extent of damages caused by the fire. This investigation is on-going.

The Governor has proposed legislation which the Illinois General Assembly is currently considering which would establish joint rulemaking authority in the three State agencies most directly responsible for telecommunications, fire protection, and emergency services. The purposes of this joint rulemaking will be to provide assurances that appropriate protective measures are in place to prevent major interruptions of the telecommunications services and to provide further assurances of a proper emergency response if such protections fail. We have provided copies of that legislation in our written testimony.

Finally, the Illinois Emergency Services and Disaster Agency is currently considering various options on the design of a system that would enable the agency to communicate with sheriffs' departments and fire departments throughout the State on a system that is not dependent upon the telephone lines.

In summary, the Hinsdale fire and its aftermath highlighted the important need nationwide for emergency planning and preparedness for the area of telecommunications, as well as other vital public services. Obviously, the continuity of telecommunications services is vital to the public and private sectors, as well as for national security reasons.

The Hinsdale fire starkly illustrated the problems which could exist in every State concerning the lack of effective emergency planning and adequate safeguards to protect their telecommunications services. Moreover, the possibility exists for a much greater failure involving more than one switching station, as in the Hinsdale incident, or even the simultaneous occurrence of incidents which could greatly multiply the adverse effects experienced. These known inadequacies should be addressed at both the State and Federal level in an expedited manner before another telecommunications failure occurs. Whether a future telecommunications failure is caused by technical failure, terrorist act or natural disaster, the Hinsdale fire has demonstrated that widespread disruption of telecommunications services could be catastrophic.

Thank you, Mr. Chairman and members of the Committee.

Chairman GLENN. Thank you very much, Mr. King. I appreciate that.

Your entire statement will be included in the record, without objection. It gives more detail of what happened there, and I would submit to other members of the committee that it would be good reading.

How many centers like Hinsdale, do you have in Illinois?

Mr. KING. Twelve or more, sir.

Chairman GLENN. And, as you understand, that would be the common practice in most States, that there would be multiple centers like this?

Mr. KING. Well, I believe in the Bell System they would be similar to this. I am not sure if the other telecommunications companies have similar services.

Chairman GLENN. Have you ever heard a figure for the whole country on the number of places like Hinsdale that would be——

Mr. KING. In my written testimony, I believe I have a number of around 11,500.

Chairman GLENN. Like Hinsdale?

Mr. KING. Yes.

Chairman GLENN. Was Hinsdale any more vulnerable than these other centers, as far as you know?

Mr. KING. No.

Chairman GLENN. When you re-did the Hinsdale center and went to fiber-optics, as you pointed out, does that make it more or less vulnerable to anything like this happening in the future?

Mr. KING. Well, it was the configuration of the wiring that caused it to be vulnerable, and that is another thing they are looked into in the report, is to reconfigure the existing wiring system, to possible make it more redundant.

Chairman GLENN. What I was wondering was, if you are using fiber-optics and going to higher numbers of calls with less equipment, perhaps it becomes even more vulnerable than it was before, but perhaps it is less vulnerable to a fire——

Mr. KING. Correct.

Chairman GLENN [continuing]. To an intentional disruption. Have you made any changes to the other 11 or so centers besides Hinsdale that you have in Illinois as a result of the Hinsdale fire?

Mr. KING. No, sir, we have not. We are waiting for the completion of the report, which is due out the 28th of this month.

Chairman GLENN. Thank you.

Senator Cohen?

Senator COHEN. No questions, Mr. Chairman.

Chairman GLENN. Thank you.

Under our early bird rule, Senator Lieberman?

Senator LIEBERMAN. Mr. King, the public around the country has really come to depend on the 911 emergency number. Maybe it is a question that answers itself, but as part of your response to this event that you have described, is there anything special that can be done to bring that 911 back on line for certain areas more quickly? Is that part of your consideration of how to deal with a crisis of this kind?

Mr. KING. Well, our agency is directly responsible for implementing the 911 service in the State of Illinois and assisting communities in implementing it. To my knowledge, you would not be able to bring the 911 service on any more quickly than your own normal telephone service. It would just be a part of that service.

Senator LIEBERMAN. Prior to this event were you, I meaning the State of Illinois, aware of the importance of the Hinsdale location to communications within Illinois?

Mr. KING. We were aware of the importance of it from a technical perspective, but we were not nearly aware of the consequences and it being as vulnerable as it was.

Senator LIEBERMAN. Did the Federal Government play any role, prior to this occurrence, to alert you to critical telecommunications or energy sectors in the State of Illinois?

Mr. KING. No, to my knowledge they have not, just what we have read in the newspaper. There has been some concern in the State of Illinois about those issues.

Senator LIEBERMAN. Was the Federal Government involved with you in the response to the crisis?

Mr. KING. No one from the Federal agencies contacted my office. I am not sure, Tom, if they contacted you.

Mr. ORTCIGER. Senator, outside of an inquiry made to Illinois Bell by the Office of the Manager of the National Communications System, we have had no inquiry from any other agencies.

Senator LIEBERMAN. So, all that you did to get back on line, and all that you have done since then to set up a system to deal quickly and effectively with a similar crisis has been accomplished from within the State?

Mr. KING. That is correct, sir.

Senator LIEBERMAN. Solely within the State. Very briefly—this is a big question and I do not want to take up too much of the Committee's time—but what advice would you give to other State or local governments about what might be done to prepare to handle a crisis of this kind?

Mr. KING. I will give that to Tom.

Mr. ORTCIGER. Well, from all of our investigation to this point, there is absolutely a need for preplanning, both between police and fire departments and the telecommunications and by the State have back-up networks of emergency communications, we believe that is absolutely necessary.

Secondly is we have been investigating, along with Bell, the possibility of having greater failure built into their system, and they are at this point considering something to that end.

We also would recommend to other States that whatever comes out of our report will probably, if it is a Bell System, have the same impact in their State.

Senator LIEBERMAN. Thank you.

Thank you, Mr. Chairman.

Chairman GLENN. Senator Roth?

Senator ROTH. I have no questions, Mr. Chairman.

Chairman GLENN. Thank you, gentlemen.

Mr. KING. Thank you very much.

Chairman GLENN. Thank you.

The next witnesses this morning are Mr. John C. McDonald, chairman, Committee on the Review of Switching, Synchronization and Network Control in National Security Telecommunications, National Research Council, National Academy of Sciences, National Academy of Engineering; and Lt. Gen. Lee M. Paschall, USAF (Ret.), Director of the Defense Communications Agency from 1974 through 1978.

Gentlemen, I understand that General Paschall will lead off for us this morning. We appreciate your testimony and your entire statement will be included in the record if you choose to give an abridged version.

TESTIMONY OF LT. GEN. LEE M. PASCHALL, USAF (RET.), FORMER DIRECTOR, DEFENSE COMMUNICATIONS AGENCY, AND JOHN C. McDONALD, CHAIRMAN, COMMITTEE ON THE REVIEW OF SWITCHING, SYNCHRONIZATION AND NETWORK CONTROL IN NATIONAL SECURITY TELECOMMUNICATIONS, NATIONAL RESEARCH COUNCIL, NATIONAL ACADEMY OF SCIENCES, NATIONAL ACADEMY OF ENGINEERING [1]

General PASCHALL. Thank you, Mr. Chairman.

I am pleased to appear before the Senate Governmental Affairs Committee on what I consider to be a very important subject. It has become almost trite to say that our society has become critically dependent upon telecommunications as we move into the information age, and at the same times our telecommunications structure has been rapidly changing and will continue to do in ways that will magnify the effects of significant service outages, whether deliberately or accidentally caused. And although both industry and government have taken some actions designed to cope with such situations, it is far from clear that those actions will be adequate in the future.

Since 1982, the telecommunications industry in this country has changed dramatically. Competition, which had a rather shaky start 10 years before divestiture in the form of private microwave radio carriers, resellers and domestic satellite carriers has greatly accelerated. Economics and the natural desire to achieve competitive advantage now drive decisions to a far greater degree than ever before in our telecommunications world.

At about that same time, a new technology emerged in the form of very high capacity fiber-optic cable systems, and when combined with the continuing progress being made in computerized telecommunications switching equipment, the telecommunications networks themselves began to change in dramatic ways.

Transmission systems in the future will be fewer in number and will carry much greater amounts of communications traffic. There will be fewer switching centers, but each will be capable of routing enormous numbers of voice and data messages. This increased concentration of telecommunications into fewer facilities makes each communications facility that much more important or that much more vulnerable. Thus, an event such as just described, the fire in the Hinsdale telephone office, had a major impact on users of telecommunications over a rather wide area and for a relatively long period of time.

Now, compounding the problem is the growing dependence of telecommunications systems on computers and their software in providing new services to customers and for managing and controlling the networks themselves. We do not yet know how to build computer programs that are completely invulnerable to penetration by outsiders, the hacker idea.

---

[1] See p. 188 for Mr. McDonald's prepared statement.

Even restricting access only to authorized users and using very sophisticated authentication and encryption schemes may fail to protect against the disaffected employee who is authorized access. It is hard to imagine the chaos which would ensue if something like last year's "November virus" were to infect the Nation's major switching center computers.

Even though our telecommunications structure is now more fragmented in a management sense and more concentrated in a technical sense, it is still tremendously robust. Competition has spawned completely new networks and systems, particularly in the intercity area. Sprint and MCI have built new nationwide systems. Domestic satellite and fiber-optic systems criss-cross the country. Value added networks such as Telenet, Tymnet and others provide richly connected data systems. In the local exchange areas, cellular telephone systems are experiencing very rapid growth, and some day cable TV systems may also provide telecommunications services.

If all of these systems and networks could be interconnected in such a way as to be mutually supportive in an emergency, there would be little to be concerned about. However, it is not clear that they can be so interconnected, much less so that they will be.

Even to a reasonably well-informed observer, there does not appear to be much activity underway to assess and correct the situation I have described, other than in the national security community.

Some companies, both users and suppliers of telecommunications services, are doing something about their own vulnerabilities. Very large users can afford to procure and manage their own dedicated systems and bypass the public networks. Those with large multipoint networks and those particularly concerned about vulnerability often use satellite transmission to connect very small earth stations located on their premises. However, even those who do so, normally use the public switched network for off-net calls and usually plan to fall back on the public network if a major outage occurs in their own system.

Normally, all telecommunications carriers have some restoral assets available, most of which is usually transmission equipment. More recently, presumably an effect of the Hinsdale incident, there have been other announcements. AT&T now provides premium, that is, seconds or minutes, restoral services for major users. NYNEX has announced a program to have a mobile switching center available to rapidly restore failed switching centers.

The National Communications System organization itself has programs under way to provide for for some interoperability among domestic communications satellites, to provide for the use of government—primarily military—assets to interconnect isolated common carrier facilities, and to provide for a national emergency telephone system.

Although these NCS programs are primarily intended for use in major national emergencies to provide critical defense and continuity of government circuits, they would be useful in lesser emergencies. In fact, the NCS does, through its National Control Center, provide telecommunications support to local authorities when disaster strikes. The NCC has full-time representation from several telecommunications carriers and it does appear to work well in emergencies. But again, its primary focus is on critical government circuits and local public safety needs.

It is not clear to me that any specific government agency is worrying about the impact on the general public and a vast community of small and medium-sized businesses of a major loss of telecommunications connectivity in today's information age, and in particular one caused by a terrorist act.

I know of no effort to catalog those facilities or types of facilities in the telecommunications infrastructure whose loss would cause the greatest impact desired by a terrorist, whether publicity, or whatever other goal might suit the twisted mentality of a terrorist group. Nor is it clear to me what government activity has the responsibility to do such and thereafter to lead and encourage systematic industry efforts to be prepared to cope with such events.

I believe your hearings will provide a valuable public service in exploring these issues and I will be pleased to respond to any questions you may have.

Chairman GLENN. Thank you very much, General.

We will have Mr. McDonald's testimony next and then we will have some questions.

Mr. McDONALD. I thank you, Mr. Chairman. I appreciate this opportunity to testify on this most critical topic, the vulnerability of our Nation's telecommunications networks to major interruptions. The committee's interest in this subject is both timely and appropriate, and I want to commend the Committee and you, Mr. Chairman, for your interest.

I would also like to note that I am pleased that my home State of Connecticut is represented on the panel.

I appear today as the chairman of the Committee to Review Switching, Synchronization and Network Control in National Security Telecommunications. While I am also an officer and a member of the Board of Directors of Contel Corporation, I do not appear here as a representative of Contel, and the views that I express are not necessarily shared by my company.

My committee was established in November 1986 by the National Research Council, the principal operating agency of the National Academy of Sciences and the National Academy of Engineering, at the request of the Manager of the National Communications Systems, NCS.

My committee was charged with the responsibility of examining the capability of the public switched networks to provide service for purposes of national security emergency preparedness, NSEP. I wish at the outset to commend the NCS for its diligence in carrying out its mission. I also wish to commend the National Security Telecommunications Advisory Committee, NSTAC, for bringing together industry and government representatives to address NSEP issues.

During the 2 years of our work, we have sought to build upon the solid work done by NCS, the NSTAC and two predecessor committees at the Academy. My written statement contains a detailed description of the committee's task, as well as the two reports we produced. My testimony today will focus upon the broader look taken by the committee at how the evolution of the public switch networks out to the year 2000 will affect network vulnerabilities in general and NSEP capabilities in particular.

We have concluded that the public networks are becoming more vulnerable to major service disruptions. In order to place the committee's conclusions and recommendations in proper perspective, I want to define for you the types of service interruptions we consider major.

First and foremost, we are concerned with damage resulting from events that cause massive loss of life. National level programs such as NETS are designed to serve government needs in such emergencies. But our committee also became concerned about the economic and social dislocations which can result from public switched network failures. Our society is growing ever more dependent upon communication facilities to support the daily operations of government and industry. The consequences of major network service losses will become far more serious as societal reliance upon communications becomes greater.

In this context, my message today is quite direct. First, our public switched networks are becoming more vulnerable to disruption because of the introduction of new technologies. Second, because of economic incentives to cut the cost of normal commercial operation, today's networks are being designed without sufficient attention to emergency preparedness.

Third, accidents, disasters, and attack threaten tomorrow's networks with more extensive damage than they did yesterday's or indeed today's integrated network. Fourth, our information society relies absolutely on smoothly functioning communications networks and thus the consequences of network failure are more severe. And fifth, we can reduce these growing vulnerabilities by strengthening existing governmental resources, improving contingency planning and deploying more robust network architectures.

Let me move from the general problem to focus on specific threats to our network. Broadly speaking, four threats endanger the public networks—acts of God, industrial accidents, deliberate attacks, and war. My written statement covers all of these, but in accordance with the emphasis of today's hearings, I will concentrate on deliberate attacks from two sources, terrorists and hackers.

Knowledgeable terrorists can mount correlated attacks against vital network nodes and do substantial damage. For instance, our domestic long-distance networks depend critically upon a very limited number of signal transfer points which could be disabled by a few well-placed explosives. In that event, a major portion of our long-distance networks would be rendered inoperable.

Computer hackers also pose an increasingly serious threat. Last November, a graduate student at Cornell inserted a "software worm" into the ARPANET data network, causing the network to be compromised. I wish to point out that ARPANET is only a semipublic network, but this example demonstrates the vulnerability of modern networks to hostile software intrusion.

Regulation, which is opening up network software to outside access, will increase the vulnerability of public networks to hostile penetration.

Let me turn to the changes in network technologies which are making the public networks less reliable providers of emergency services. Three technologies are heavily influencing the future architectures of networks: Fiber-optic cables, digital switching, and software.

While each of these technologies bring substantial benefits to network users, each also creates or amplifies network vulnerabilities. Increasingly, fiber is becoming the transmission medium of choice for most telecommunications. The economics of increasingly competitive telecommunications markets are driving network designers to concentrate more and more communication channels into a single fiber, leading to future reductions in physical redundancy, which has historically characterized public networks.

By 1995, the long-distance network will be almost exclusively fiber. As fiber supplants copper cable, microwave radio and satellites, network transmission is being deprived of media diversity, a valuable means of backup communications. Also, fiber routes selected by competing carriers tend to be physically co-located. Geographic barriers, such as mountain ranges and rivers, impose natural constraints on the selection of routes for communication lines. For example, a single bridge may frequently carry fiber cables from many communications suppliers. Also, fiber rights-of-ways tend to follow railway and highway routes.

A second trend in technology which is amplifying network vulnerabilities is the widespread deployment of digital switching in public networks. In the past, the sheer size and cost of electromechanical systems has limited the number of calls which could be routed by a single system. Digital switching systems are compact and can economically serve two to five times as many customers as their analog counterparts.

Many digital switches are being employed as remote nodes linked to larger host switches, and the economics of switching will drive network topologies toward greater traffic concentration in megasize central switching nodes.

The final worrisome trend is the greatly increased reliance on the network upon software to control network operations. This software is becoming increasingly accessible to the public to deliver new network services, permitting customer defined network service features. Sophisticated software is also a source of vulnerability in modern network signaling.

The purpose of signaling is to route a call through the network and establish a conversation path. In old systems, signaling was "in-band." The network signals were carried over the same channel as the conversation. In the new signaling system, signaling is carried over a separate network containing far fewer transmission paths. This new signaling technology provides much flexibility in processing and routing calls. However, the concentration of the signaling software and hardware into a subnetwork means more vulnerability than if the signaling function were spread throughout the entire networks. Without signaling, networks cannot function, so this added vulnerability is a serious matter.

Another source of software vulnerability lies from the trend towards national data bases. Some of the intelligence which would normally reside in the local switching office is now removed and concentrated at a distant point accessed by the signaling network. There will only be a few of these data bases.

The committee was briefed by the FCC on their network access concept called open network architecture or ONA. ONA allows entrepreneurs to create services which compete with local exchange carriers' offerings by accessing the software in public network switches. While such open access fosters competition, it also could give hostile agents increased opportunities to damage the public networks by altering data bases or possibly overloading network computers. Simply put, more people will have access to network software and they will know more about how to manipulate it.

I should note that the enormous proliferation of private networks will not alleviate these problems. Such networks employ the same technologies, and unless they are interconnected and interoperable with the public networks, they do not provide much redundancy. Indeed, many of these network lines interconnect with the public networks through hubs like Hinsdale, and often their lines are derived from public network facilities.

In any event, private lines between business offices will not help a resident who needs immediate access to 911 service after a central office burns down.

What needs to be done? Here, I would like to highlight for you some of the committee's recommendations for enhancing the NSEP capabilities of the public switched networks. I will emphasize those recommendations which speak to the role that the Federal Government can play in this remedial process.

Government must be able to analyze what network features are necessary for national security. Government must also be able to implement plans and procure services pertinent to national security needs. In its efforts to date to evaluate the NSEP capabilities of the public networks, the Federal Government has not considered how network capabilities might be enhanced to reduce vulnerabilities to broader economic and social disruption.

Our committee has concluded that there is a gap in NSEP oversight. We believe that the government should review whether its existing resources are sufficient to adequately perform expanded NSEP oversight of the proliferating public networks, and clarify the appropriate agency missions to address these broader NSEP questions.

Next, trends in technology are increasingly concentrating public network assets in a few dominant technologies which I have discussed today, fiber, digital switching and software. The committee finds that these trends could adversely affect NSEP, and recommends action to make critical network nodes more secure, reduce the concentration of network traffic, and examine ways to provide more diversity in transmission facilities.

A third vital step to enhance NSEP is to augment existing crisis management capabilities. For emergency services to be effectively delivered, it is important to plan ahead. The day after an earthquake is no time for original research in crisis management. The government should establish additional emergency plans, tailored to the evolving public networks, which use simulated disaster and recovery scenarios to develop fallback strategies for network use during emergencies, for example, protection and backup of vital network nodes.

Perhaps the most disturbing of these growing network vulnerabilities is that of increasingly open outside access to network data bases. The desire to open access to the public networks must be counterbalanced by the recognition that the integrity of these networks must be protected. The government should address how to protect the public networks from penetration by hostile users, especially with regard to harmful manipulation of any software embedded within the public networks which is open to customer access for purposes of network management and control.

We will make these and other recommendations in our Phase II report to our sponsor, the National Communications System. We will not make specific recommendations as to how they should be implemented, however. Such advice would go beyond our committee's charter.

In conclusion, the public networks are becoming more vulnerable to major disruptions. Recent events such as the Hinsdale fire demonstrate the increase in magnitude of service outages. The spate of computer viruses graphically demonstrate the growing potential for misuse of our communications networks to damage vital software data bases. In our view, these events could be harbingers of even more serious disruptions that could occur in the 1990's.

The vulnerabilities stemming from network technology are not significantly offset by any countertrend. Robust systems such as NETS will be necessary to enable the government to carry out vital NSEP responsibilities. Civil emergencies will also require enhancements and backup to the capabilities of networks whose architectures are being driven primarily by economic incentives, rather than by security concerns.

As I noted earlier, our information society is increasingly dependent on the smooth functioning of our information highways. Residential users need 911 service and will increasingly rely on the "smart home" data services, such as alarm monitoring and energy management, business users—notably the international financial community—cannot run their enterprises without enormous volumes of voice and data devices, and at the same time these concerns apply for government users.

I believe that we must act now to reduce the network vulnerabilities I have described in this testimony. I have today cited some of our committee's major recommendations for enhancing emergency service capabilities to the public switched networks. Other recommendations are presented in the committee's forthcoming report, and if it pleases the Committee, I will be happy to make copies of the full report available to you as soon as they are available.

Chairman GLENN. We appreciate that.

Mr. McDONALD. Critical to the effectiveness of our report and its recommendations is a sense of urgency which I hope that these hearings and your Committee may help instill.

Thank you, Mr. Chairman and members of the Committee, for your interest and for this important opportunity to testify here today.

Chairman GLENN. Thank you very much, Mr. McDonald. On page 8 of your testimony submitted to the Committee, you talk about the example of "Captain Midnight". In effect it concerns capturing a satellite and putting out spurious signals or programming of your own design, I guess we could say, on that particular channel. This indicates, to some extent, what you can do with a well-placed hacker trying to get into the system some place.

I am also concerned about computer controls that control electrical grids, oil supply lines, gas supply lines, and things like that. Are there any examples you know of where the hackers have gotten into these controls of our energy systems?

Mr. McDONALD. Speaking for my committee, we did not really discuss the power grid, except as outages would relate to the central offices if they lost power. What we found there was that losses of power could be accommodated for a period of days, because of the oil supplies and motor backups that exist there. But to answer your question specifically, we did not study the controls of pipelines or the power grids.

Chairman GLENN. General, do you know of any instances where the hackers have gotten into these other control systems, do you know?

General PASCHALL. None to my knowledge, sir, but I am not an expert on the power grid and how it is operated.

Chairman GLENN. Mr. McDonald, on page 8, also at the bottom of the page, you say, "A few well-placed hand grenades would crash major portions of the domestic long-distance networks." I want to be sure I understand your testimony on that. You are saying that a very few, well-placed hand grenades could crash the entire AT&T network. Is that right?

Mr. McDONALD. We studied the long-distance networks in great detail, and in our report, our first report, we describe the sensitivity that you have cited, and that is exactly right.

Now, I understand subsequently to our first report that there have been some modifications made to the network and my committee has not been briefed on those modifications. But at the time we made our first report, that indeed was the case.

Chairman GLENN. Would these be situations where someone with a hand grenade, if you want to use that example, would have to obtain access into the heart of a certain facility. Could that damage be done externally by a hand grenade?

Mr. McDONALD. No, that damage would have to be done to a switching system which would be located in a building and there would be some form of security there. But indeed, if they all happened at the same time in a correlated event, all of that carrier's network would be disabled.

Chairman GLENN. Would the same be true for Sprint and MCI?

Mr. McDONALD. We have not been briefed specifically on Sprint and MCI, but the technology is being applied in the same way and I believe that a similar situation does occur with those carriers.

Chairman GLENN. General, do you feel that, since the days when you were managing the National Communications Service and Defense Communications Agency, our situation has become more vulnerable or less vulnerable?

General PASCHALL. I believe it has become more vulnerable and, for the reasons given in my statement, it is the technology that is both concentrating our assets and the divestiture which is spread-

ing out our management. These problems used to be much easier to handle when you had a single unified Bell System and the government was more able to influence decisions based on public interest, rather than competition and economics.

Chairman GLENN. Through the modified final judgment breaking up AT&T, DOD was able to require the regional local phone monopolies to commit significant resources through its common operating arm, Bellcore. These expenditures for national security emergency preparation, NSEP as it is called, for Bellcore alone are almost a billion dollars a year. Other companies are also making more or less mandated expenditures. Is that adequate to do the job that needs to be done?

General PASCHALL. Well, sir, I am not an expert on Bellcore. I know why it was established and I know what it does. I would be very surprised if Bellcore spends a billion dollars a year on NSEP, national security emergency preparedness matters. I would suspect it is a very much smaller amount than that.

The key point of your question is how much should be spent. The NSEP expenditures thus far for the communications satellite interoperability program of the NCS and for the NETS programs—that budget is just now being put together, as I understand it—are significantly less than a billion dollars a year.

My own personal guess is that the systems and networks are so robust that if we were to find ways to interconnect them and interoperate them, that it should not cost that kind of money. It is finding the right leverage points and doing the relatively small things that need to be done, and I know of no technical reason why these cannot be done. There are competitive and proprietary policy reasons why it is going to be quite difficult to do.

Chairman GLENN. I know my time is up, the red light is on there, but just one additional question. You played a role with NCS and DCA, national communications as well as defense. Is there somewhat of a Mutt and Jeff relationship in having NCS, the civilian component, folded into such a larger agency?

General PASCHALL. The Director of DCA, as you note, is the Manager of the National Communications System as well as the Director of DCA. I found it worked well. The DCS, the Defense Communications System, provides about 80 percent of the assets used by the National Communications System, and were I the manager of NCS outside, I would much prefer to have my largest supplier on my side, rather than an opponent. From a pure politics standpoint, it would work better that way.

I found the other operating components of the NCS to be cooperative and I do not know where else I would put it, were I given the choice of putting it somewhere else. It seems logical to me.

Chairman GLENN. Do you have any comments on that, Mr. McDonald?

Mr. MCDONALD. I am not an expert in government, sir. I will pass.

Chairman GLENN. Senator Lieberman?

Senator LIEBERMAN. Thank you, Mr. Chairman.

In listening to you, maybe we need some non-experts to come in and render some advice about what government should do. I must say, as I listened to the two of you—and I thank you for your excellent testimony—in the quiet discourse of this Committee room, in thoughtful and methodical words, you are really making a powerful statement. As I hear it, it screams out for further attention. You are saying quite clearly that there are events occurring,—technological developments and economic developments, natural competitiveness, economic motivations in the telecommunications industry—that are, if I may use the term, naturally conspiring to make the system more vulnerable.

Accept for a minute that we have a system that is growing more vulnerable; unfortunately, real world events tell us that there are people out there who will not play by the norms and rules of civilized human behavior who will take advantage of those vulnerabilities. We do not need any more compelling or fresh example than the planting of the bomb on Pan Am Flight 103.

Faced with vulnerability and a world in which people will be lawless, I do not have a sense from today's testimony that we are moving to shore up our defenses, to lessen our vulnerability either within or outside the government. I am troubled by your compelling statement, General, that we are more vulnerable today than we were when you were in charge of that telecommunications system.

Let me ask this question, perhaps to bring it home. Let me assume, as a bad case scenario, that a series of well-placed explosives go off in and around Connecticut and there is no telephone service in the State. Do you have any confidence that the people responsible within State government and within the telephone system in the State would know what to do—to establish lines of communication, for instance, with the Federal Government officials authorized to take action here?

General PASCHALL. Yes, sir, I believe so. Over the years, extending as far back as the Alaskan earthquake, almost weekly or monthly since then, a natural disaster occurs somewhere in the United States, whether Hurricane Camille, Three Mile Island, Mount Helena, and there is a method whereby the State authorities can call upon, generally through the GSA Regional Office, help and support from either FEMA, Federal Emergency Management Agency, or the NCS activities.

Indeed, I see Mr. Morriss on your witness list, and when Mr. Morriss testifies, he is much more current than I am about this. So, this happens day in and day out, on a monthly, yearly basis.

Senator LIEBERMAN. General and Mr. McDonald, would you say that the consequences of a terrorist attack on the telecommunications system would be qualitatively or quantitatively different than the impact of a natural disaster that interrupted telecommunications?

General PASCHALL. I make a distinction, and it may be too fine a distinction, in my written statement about the target set that a terrorist might choose. The National Communications System organization has looked at national security and emergency preparedness types of target sets.

Natural disasters are acts of God and they produce their own targets. A terrorist target set might be quite a different thing. They could be very, very precisely defined for maximum publicity or to hit something or they did not like in the capitalist system, Wall

Street or something like that. It is that area that I do not see much effort underway.

Senator **Lieberman**. Mr. McDonald?

Mr. **McDonald**. Could I back up for one minute to your first question?

Senator **Lieberman**. Surely.

Mr. **McDonald**. I would like to add my two bits worth on "is preparedness there." What would happen in Connecticut if the telephone service was hit, are there preparedness plans there?

I was in Connecticut when Gloria came through, and I am a ham radio operator so I began to get onto the networks of ham radios in case all the telephones went down, and indeed I do feel that the Nation has the ability to plan for events that they have seen before, earthquakes have happened in California, hurricanes happen, and I really feel that the State was prepared for major outages in telecommunications.

When it comes to events that we have not planned on—the Hinsdale fire which I think you heard earlier, the preparation was not there. Our committee feels that there is not adequate preparation when it comes to major telecommunications outages such as Hinsdale, that there is no forewarning and we recommend strongly that there be simulations done, that there be plans made ahead of time to accommodate these disasters.

Senator **Lieberman**. That would include, I assume, planned intentional terrorist attacks occurring?

Mr. **McDonald**. Exactly, and that would relate to your second question, that a terrorist attack can be done. I mean the information is public knowledge about the sum and substance of the telecommunications industry, and I think the planning that could be done that would allow us to be more prepared for Hinsdale would indeed also help us in the case of a terrorist attack.

Senator **Lieberman**. And I take it that the lack of preparedness or the need for more preparation and planning that you have cited would go both to public and private entities, is that correct?

Mr. **McDonald**. That is correct.

Senator **Lieberman**. If I may, Mr. Chairman, while we are on this trend, ask just one last question. I was struck by the testimony of the gentleman from Illinois that there was no Federal Government involvement in that crisis. Were you surprised by that, General?

General **Paschall**. Yes, sir, and I think perhaps—well, it may be that the Federal Government's involvement was preplanned in the sense that the Government's critical circuits, the VA, the FAA and such as that, have assigned restoration priorities in advance, and the telephone companies would have been restoring those circuits in accordance with that restoration priority scheme.

Typically, the NCS, or at least when I was there as the manager, the NCS does not intervene except on request from the State authorities, except as it pertains to those circuits that have been designated as priority circuits and, hence, have a priority restoral already established with the common carriers.

Senator **Lieberman**. My time is up. I will return for a few more questions after Senator Glenn.

Chairman **Glenn**. Thank you.

General, would you agree with Mr. McDonald that there is a gap in NSC oversight? They have prime responsibility in this area, and FEMA has some other responsibilities. Mr. McDonald felt there was a gap in NSC's oversight and more should be done. Do you agree with that?

General PASCHALL. I do not know of anyone who is specifically concerning themselves with terrorist activities, and to that extent, yes, there is an oversight. As to which agency ought to do it, I am a little skeptical of assigning such a task to the NCS staff, which concerns itself primarily with critical government circuits and national security affairs. The expertise may not be there to deal with general public and public safety affairs on a local level, which maybe FEMA or it could be the FCC's responsibility to require some of these actions be taken by industry themselves.

Chairman GLENN. Well, I was talking about the National Security Council. We get mixed up in our initials here. NCS and NSC. You mentioned the Federal Communications Commission, and it appears that they have the authority to do quite a number of things if they wanted. Are they making adequate use of their authority to get into this area?

General PASCHALL. I have not seen that much evidence of it, Senator. They do issue the rules that were prepared by the National Communications System activities for restoration priorities, the so-called telecommunications service procedures.

Chairman GLENN. I think all of us thought for many years that just the very diversity of our system, whether it was in communications or in energy or gas pipelines or oil or electrical grids or whatever, that just the very diversity of these systems had protected us. But I think what we are learning is that the trend toward new technologies and more and more centralized control is making us more vulnerable. I do not think we have moved to take that into consideration enough.

General PASCHALL. Exactly.

Mr. MCDONALD. This was one of the committee's major thrusts and we decided to look into the future. We decided to say let us try to examine what the network will look like in the year 2000 and then assess the emergency preparedness situation at that time, and that is when we became alarmed and that is what has led us to our recommendations. There have not been events to date that one would consider a national disaster. Certainly, Hinsdale, as you pointed out in your opening comments, was not a national disaster. It was a bad event, but it was a regional and local situation. But what we see as we project into the future is quite alarming.

Chairman GLENN. Senator Lieberman?

Senator LIEBERMAN. Thank you, Mr. Chairman.

General, we talked before about State and local officials and executives of telecommunications companies on the scene. Are you—and Mr. McDonald, too—confident that they know enough about the Federal system to be in touch with GSA, with FEMA, or with other Federal agencies involved? Are they sufficiently briefed and alerted?

General PASCHALL. Senator, I served on the two predecessor committees to the one that Mr. McDonald now heads. In the committee once removed in the past, we had extensive dialogue with State and local authorities. We dealt with the governors group and such as that.

Other than the fact that there is someone who always does not get the word, yes, sir, I think the States do know they have available to them this asset. Whether or not they choose to call upon it, of course, is a State or local decision.

Mr. LIEBERMAN. Mr. McDonald, from your work, do you think that there is a need—this follows up on the question that Senator Glenn asked before—for one Federal agency to have responsibility for dealing with the vulnerability of our telecommunications network to terrorist attack?

I must say, as I read the report by Mr. Lane for the Committee, there really is a maze of Federal acronymned agencies at work here. Is it being properly coordinated? Should we focus it somewhere?

Mr. MCDONALD. I do not think it is being properly coordinated. One of our conclusions—we had briefings by a large array of government agencies, and the NCS is doing a marvelous job in their planning for activities that relate to massive loss of life.

When it comes to the areas of economic disruption or social disruption, we feel that more needs to be done, and our report will recommend that.

Senator LIEBERMAN. Maybe I should wait for the report. I was going to ask you whether you thought an existing agency could play that role, or is there a need for the creation of a new agency?

Mr. MCDONALD. My committee is not an expert in how you manage the Government and, as I mentioned in my oral testimony, we will not attempt to make implementation recommendations.

Senator LIEBERMAN. Let me go to another part of the testimony of both of you—the effect of technological developments and economic competition in removing what we are calling redundancy. Redundancy, I gather, basically means the existence of a lot of different ways to do the same thing, so if we lose one or two facilities others remain. As this continues, and particularly as we rely more on fiber optics, the natural forces of the market and technology increase our vulnerability. Is there a new role for government here to provide essentially a broader network of fallback systems, perhaps alternate systems, such as satellite means of communication?

Mr. MCDONALD. I think there is. I think that there is need for government in a number of areas. First of all, I think there is a need to create the planning that can be implemented when a disaster strikes. I think that critical nodes need to be identified, that simulations need to be made, and that plans need to be in place to prepare one for an emergency. After it happens is no time to start thinking about it, so I do feel that the government could take that role.

I think government also, when they recognize the trends and see a trend that you gentlemen might perceive as unfortunate, that there are other technologies that can help the situation, technologies such as very small aperture earth stations, the VSATs, using satellites, technologies such as radio access, using cellular mobile radio, and use of packet switch network. Those are three technologies that are emerging and I think with the proper emphasis their use could be more widely deployed.

I think NSTAC is a good one to hear the concerns of government and then to take the appropriate actions.

Senator LIEBERMAN. You anticipated my next question. I was thinking that one technological development that may help us deal with the threat of terrorist attacks may be the cellular telephones, mobile telephones, which by virtue of market forces are spreading pretty rapidly themselves, is that correct?

Mr. McDONALD. That is correct, but indeed one has to consider the attack. I do not think it was mentioned in the testimony from Illinois, but there was a cellular mobil telephone switching office in Hinsdale that was also consumed, and so if you put all the eggs in one basket and the basket gets dropped, everything goes.

Senator LIEBERMAN. Thank you.

Chairman GLENN. Just a couple of comments. Every time we think we have about gotten to the limit of telecommunications advances, new things happen. I think we tend sometimes to think if we just solve our situation now, everything will be fine. You know, "everything is up to date in Kansas City, we have gone about as far as they can go," that attitude, and yet we find enormous advances coming one after the other.

I do not know what role the Federal Government should play in this area, quite frankly. I am very concerned about it. I do not want to play "big brother" and put a lot of requirements out there. But when we have an industry that is going ahead as rapidly as this is and we see new vulnerabilities developing, we get ourselves into a real quagmire as to what we should do or should not do. We see the vulnerabilities which are being spelled out to some extent here this morning, and then what do we do about it? We can advise, but you are dealing with a highly competitive industry and you are dealing with people out there who, if you lay Federal rules and regulations on them about what they can or cannot put up or the siting of things or the vulnerabilities of which they have to take account then you add expense to their business operation and there you are. Perhaps you put them out of business in a highly competitive industry.

So, I do not know where we go with this. I think advice is one thing. But if I was sitting out there as a hard-headed business executive trying to make a decision, required to spend an extra $10 million for a switching site that I did not think was going to add anything to my production or my capacity, yet was going to make it less vulnerable to some terrorist attack that I was not scared about to begin with, then I am going to probably object. That is the problem we face here, and that you face in the advisory capacity, as you have in the past, too. I do not ask that as a question, I just make it as a statement.

General PASCHALL. There is one thing the government can do and indeed has done, and that is to use its economic power. The government is a large buyer of communications services from the common carrier industry, and in one instance the government did issue a policy a couple of years ago that said, because of a certain vulnerability of communications satellites, that communications satellites that were not protected from that vulnerability and launched after 1990, the government would not use service over those satellites. That did encourage at least two, and a third that I am aware of, satellite company to put a protection feature onboard, simply to avoid the loss of government business.

Those kinds of things can be done, where you use your economic power, but is very hard, as you say, to try to inject yourself into the commercial businesses' decisionmaking process.

Chairman GLENN. And if we see vulnerabilities creeping in, we cannot afford to stay out of it when if we are looking at the national security.

Thank you very much, gentlemen. We have another panel here. I appreciate your being here. Thank you much.

Our next witnesses are Mr. Thomas A. Norman, Vice President of Engineering and Operations, United Telecommunications, Inc., representing the National Security Telecommunications Advisory Committee; and Mr. Benham E. Morriss, Deputy Manager of the National Communications System.

Gentlemen, we welcome you this morning and look forward to your statements in abridged or full version. In either case, your entire statement will be included in the record.

Mr. Norman, if you would lead off, please.

TESTIMONY OF THOMAS A. NORMAN, VICE PRESIDENT OF ENGINEERING AND OPERATIONS, UNITED TELECOMMUNICATIONS, INC., ON BEHALF OF THE NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE;[1] AND BENHAM E. MORRISS, DEPUTY MANAGER, NATIONAL COMMUNICATIONS SYSTEM[2]

Mr. NORMAN. Mr. Chairman and distinguished members of the Committee, my name is Tom Norman. I am vice president of Engineering and Operations of United Telecommunications, Inc. or United Telecom.

United Telecom is a telecommunications holding company, with subsidiaries that provide a wide range of telecommunications services and products and data processing software services. The chairman of United Telecom, Paul Henson, is currently chairman of the National Security Telecommunications Advisory Committee or NSTAC, and I am his representative on the Industry Executive Subcommittee.

Having spent the first 40 years of my life living in Ohio and the first 20 years of my telecommunications career with the Ohio Bell Telephone Company, I am particularly honored to come before this Committee and the Chairman of this Committee. I have 27 years of experience in the industry at the local exchange level and engineering, planning and the maintenance of telecommunications networks.

I have submitted testimony that you have before you and, in the interest of time, I will speak to the highlights of that written statement and then be available for questions.

In 1982, recognizing the diverse structure of the telecommunications industry that provides national security emergency preparedness or NSEP telecommunications services—and anticipating the Bell System divestiture—as well as the need for cooperation among industry participants in meeting NSEP needs, President Reagan formed the NSTAC.

---

[1] See p. 207 for Mr. Norman's prepared statement.

[2] See p. 229 for Mr. Morriss' prepared statement.

Established by Executive Order 12382, the NSTAC provides expert advice and assistance to the President. Pursuant to that Executive Order, the NSTAC is composed of up to 30 members, appointed by the President from the senior executive ranks of the Nation's leading telecommunications companies.

The NSTAC provides the telecommunications industry's perspective on the survivability of NSEP telecommunications services and suggests enhancements, where appropriate. In its endeavors, the NSTAC is supported by an Industry Executive Subcommittee, which consists of an executive appointed from each NSTAC company. The IES establishes industry task forces and working groups to pursue issues of particular NSEP telecommunications interest or concern.

In carrying out its functions and duties, NSTAC conducts reviews and assessments of the effectiveness of national security telecommunications policy. The NSTAC periodically reports to the President and to the Secretary of Defense (in his capacity as Executive Agent for NCS).

The NSTAC is designed to serve, and indeed does serve, as the government's link to the telecommunications industry with respect to NSEP telecommunications. It also provides a forum for joint industry/government national security telecommunications planning.

As a result of the FCC's Computer Inquiry II decisions and the divestiture of the Bell Operating Companies from AT&T, the Federal Government no longer had a de facto single manager for end-to-end telecommunications services. Thus, one of the first issues considered by the NSTAC was the ability to coordinate the response of the various telecommunications vendors and carriers in the event of an emergency situation.

In July 1982, a National Security Telecommunications Conference, attended by senior industry and government representatives, gave priority to joint network planning. At the inaugural meeting of the NSTAC in December 1982, the National Coordinating Mechanism Task Force was established.

That task force addressed the need to coordinate and link the operations centers of major telecommunications carriers with the government's operation centers. The NSTAC recommended to the President that priority be given to creating a mechanism for reconstitution of telecommunications capabilities in case of emergencies. The resulting mechanism would be the center of the Nation's capability to harness telecommunications in response to any national crisis.

Building upon this framework, the NCM Task Force recommended initiatives that included the establishment of a joint industry-government National Coordinating Center or NCC. The mission of the NCC is to assist in the initiation, coordination, restoration, and reconstitution of NSEP telecommunications services and their supporting facilities. That mission is accomplished through a unique organization staffed, operated, and funded by both the Federal Government and private industry. The goal of the NCC is to assure that the Nation's telecommunications resources are available under all emergency conditions, including war.

The representatives assigned to the NCC are knowledgeable of their company's or agency's system. In an emergency or crisis situation, the NCC will determine the extent of damage and the steps necessary to restore telecommunications services. In this regard, each representative maintains lists of contacts within the parent organization in order to know whom to call on, as well as an inventory of equipment available for emergency use.

In addition to their coordinating mission, NCC representatives work together on a day-to-day basis to prepare plans and procedures to deal with major disasters and emergencies ranging from fires, floods, and earthquakes, to a nuclear attack on the United States.

The industry representatives work with the government representatives to determine which essential Government telecommunications services can be restored and the priority of each. That mutual effort will result in more efficient and rapid restoration of telecommunications than if the Government dealt individually with each company.

The NCC has responded during real emergencies such as Hurricane Gilbert, the Cuban prisoner riots, and the fires in the Brooklyn, New York and Hinsdale, Illinois central offices. It has also supported the U.S. Customs Service and the U.S. Coast Guard in drug interdiction efforts in South Florida, and has operated during the earthquakes in Coalinga and Palm Springs, California.

NCC member companies have also supported certain Presidential and Department of Defense telecommunications requirements, including the provision of communications for United States and Soviet inspectors under provisions of the INF Treaty.

That the industry members of the NCC provide representation at their own expense is noteworthy.

The process used in creating the NCC from the very first has been applied to a number of issues brought before the NSTAC, that is, identify an issue, assign it to a task force made up of industry and government representatives with the appropriate subject matter experts, and after a complete investigation, recommendations are made and actions taken.

The NSTAC is currently assessing a number of issues on active task forces or working groups. They are commercial satellite survivability, telecommunications systems survivability, telecommunications industry mobilization, telecommunications service priority, national telecommunications management structures, and energy.

Representative of the type of industry-government cooperation that can take place is the work on telecommunications service priority or TSP. The TSP System is a priority system for ordering the Nation's most important NSEP telecommunications services. The TSP System authorizes and requires telecommunications vendors to both provide new NSEP services and to restore existing NSEP services before all others. The TSP Task Force is to assist the NCS as it implements the TSP System by making recommendations for those aspects of the TSP System most directly affecting the telecommunications industry.

Since 1967, the NCS has administered the Restoration Priority or RP System. Vast changes in the telecommunications industry, along with problems with administering the RP System, have created a need to implement a more modern system. The TSP System was developed both to address these problems and to take advantage of emerging technology. On November 17, 1988, the Federal Communications Commission authorized the new TSP System.

The TSP Task Force continues to provide advice and assistance to the NCS in conceptualizing and designing a system setting priorities with respect to the initiation and restoration of NSEP telecommunications. The task force's intent is to assist the NCS in developing a system that is not only fully responsive to NSEP requirements, but which also minimizes the impact on internal company operations, ensures effective system administration, and recognizes the varying requirements of TSP service users.

The NSTAC has proven to be an outstanding example of how government and industry can cooperate effectively to address issues of utmost importance to the Nation. It is a process that is in place and functions well.

From the industry standpoint, the NSTAC is an excellent forum to bring together the diverse interests of different companies so that our national security emergency preparedness telecommunications are advanced. The NSTAC stands prepared to address, in a timely and effective manner, new initiatives and issues in its area of expertise and responsibility.

In the event that this Committee or any other government or industry body believes that an issue exists that is not being addressed today, the NSTAC urges that the issue be brought to its attention. We have a National Coordinating Center in place to respond to any NSEP need, and we have an industry poised to be responsive in cooperation with the government.

In sum, the NSTAC is functioning well and welcomes increased use, if need be. A recent survey of the NSTAC members showed that they totally support the process. A letter dated July 11, 1988, from President Reagan, praised NSTAC and urged his successor to continue utilizing the NSTAC with respect to these vital national security concerns.

This completes my statement, Mr. Chairman, and I will be glad to take questions later.

Chairman GLENN. Thank you very much, Mr. Norman.

We will hear from Mr. Morriss first, and then we will question. Mr. Morriss?

Mr. MORRISS. Mr. Chairman and members of the Committee, I am Ben Morriss, Deputy Manager of the NCS.

Let me say that I am pleased to appear in response to your request to discuss the National Communications System's national security and emergency preparedness programs. When you go last, either everything that is worth saying has been said or you have been set up somewhere, so let me go over my testimony fairly quickly, because a lot of has already been said by previous speakers.

The National Communications System, the NCS, was established in 1963 by President Kennedy, as a result of some communications difficulties from a Federal point of view during the first Cuban missile crisis.

The charter, very simply, is to provide the Federal Government the necessary national security emergency preparedness communications under all conditions. The mission was further defined by both President Carter and by President Reagan and consummated in Executive Order by President Reagan approximately 5 years ago.

While our mission does not cover all private communications, but it does cover the support to the State and local governments for emergency preparedness, and I will say a little more about that later on. I will use the term NSEP as a shorthand for National Security Emergency Preparedness, as some of my predecessors have done.

From an organizational point of view, the NCS has an Executive Agent which is the Secretary of Defense. It has a manager, which is also double-headed as the Director of the Defense Communications Agency. They consist of 23 agencies and the communications assets of those agencies, and a managing body, a Committee of Principals, which are by and large the chief communicators of each of those governmental entities.

The Manager is charged with developing plans to handle emergencies, programs to minimize NSEP disruption from damage, tests and exercise of procedures and standards to facilitate inter-operability.

It is important to note that the NCS is a confederation, and neither the Executive Agent nor the Manager has directive authority over its members.

Because of our very large reliance on commercial communications in this country, in fact a great majority of the government's communications are leased communications—and only a very small part of it are government-owned in this country, and that is a matter of national policy—industry assistance in light of developing competition and the break-up of the Bell System was recognized as being required some time ago, and as a result of that the President did establish the National Security Telecommunications Advisory Committee, which Tom Norman spoke to just a moment ago.

Let me address the vulnerability, as I see it, of the Nation's telecommunications resources from a national security emergency preparedness point of view. The national network is quite robust. It consists, on a national point of view, of several independent networks, diverse and redundant transmission facilities and switches, and thus at the national level major disruptions during a peacetime emergency or disaster would be highly unlikely.

Absent a major regional disaster such as an earthquake or hurricane, regional telecommunications are similarly protected from major disruption from isolated incidents.

Incidents involving a single local exchange area such as Hinsdale can seriously disrupt commercial and residential services that area, but there is a history of fairly rapid restoration of most services and the special national security emergency preparedness services.

For example, in the Hinsdale situation, a majority of the FAA service is provided through the Hinsdale region were restored within 16 hours, and the FAA reported no significant impact to air traffic control in the Chicago area after the first two days.

While not feasible economically for small businesses or homes, there are a number of services that are available to industry or to the government to make their services more robust. These services available consist of things such as connection to more than one end office or have a service from more than one long-distance carrier, or a bypass for the local exchange carrier. Those things are used by some of the large companies and they are used by the Federal Government and presumably by State and local government also, but, as I say, it does not solve the problem of the homeowner when he needs to call the fire department and his local office is out.

While the NCS and the National Coordinating Center, the NCC which the NCS operates with the industry—and which I will say more about later—is not responsible for all telecommunications services in an area, they do facilitate restoration of emergency services beyond those of the Federal agencies.

For example, the Hinsdale fire also disrupted services for the North American Electrical Reliability Council Coordinating Center. Working with the Department of Energy, the NCC identified those circuits which were critical for the monitoring and management of the national power grid. These circuits would, if qualified for priority restoration under the FCC's rules and the NCC accelerated the restoral actions by authorizing the carrier to proceed with priority restoration.

Notwithstanding the strengths of the nationwide telecommunications networks, the NCC, working with the industry, is pursuing a number of activities to further enhance the survivability of these networks or to accelerate restoral, if damaged. Let me address just a few.

One of the first is addressed by the President's Advisory Committee, with the need for a national coordinating mechanism. The National Coordinating Center was created to meet this need and its mission is, as previously stated, to assist in the initiation, coordination, restoration and reconstitution of the NSEP telecommunications services or facilities, is jointly manned by both government and industry. Twelve industry representatives from the major carriers are there, provided by their own companies' expense. Those industry members all carry beepers and they are backed up. We have a recall mechanism, which is the Defense Communications Agency's operating center, so that they can be called back any time day or night.

They have operated 12 straight days, 12 hours on, 12 hours off, with their backups during exercises in the past, so we do view it, although it normally manned 8 to 5, as a 24-hour-day, 7-day-a-week facility because of its backup provision.

With respect to restoral, critical telecommunications services have for a number of years been identified to the carriers as priority restoral actions. This restoration priority system is being revised in light of the changes in the industry and the technology. The FCC has just completed a rulemaking and the new system will be operational in early 1990, which is called the Telecommunications Priority System.

The NCS has also developed procedures to permit priority provisioning of new services in an emergency. This has been used in situations such as the takeover of the Federal prisons by inmates. We operate these priority systems under the authority of the FCC, and they would certainly be applicable to respond to any terrorist activity.

We have a plan called the National Plan for Telecommunications Support in Non-Wartime Emergencies. It has been approved by the Executive Office of the President and it serves as a basis for planning in the Federal Government for the planning and utilization of regional telecommunications assets in a non-wartime situation.

The plan sorts out the responsibilities of the different government organizations in emergencies. For example, the GSA Regional Communicator operates as the NCS Regional Manager and coordinates the Federal emergency telecommunications response, that is, he operates as the Manager or the NCS's man in the field.

The emergencies beyond the capability of the regional structure, even with the additional support that can be provided from the NCC, a higher level mechanism is available. A Joint Telecommunications Resources Board has been established by the Director of the Office of Science and Technology Policy to assist him in non-wartime functions assigned by Executive Order.

Approximately 9 months ago, we held an exercise for that particular office, the Joint Telecommunications Resources Board, and the scenario for that was a terrorist activity.

The NCC has in place procedures for alerting the telecommunications industry of changing Federal alert conditions. In the case of emergencies requiring the redeployment of telecommunications resources from one part of the country to another or from one company to another, procedures exist within the NCC for coordination of military airlift missions for the deployment of other pertinent military support resources.

The NCS and the NCC are chief participants in the Federal Government's exercise program. We work closely with the Department of Defense and the Federal Emergency Management Agency on planning for and implementing major national and international exercises, and in the past year an increasing number of these exercise incidents that involved terrorism and sabotage have been planned and played by an expanding number of departments and agencies.

We also work with the States. During a recent State of California earthquake exercise, we worked out the plans and the procedures so that the California National Guard and Reserve units could use their tactical equipment to restore some seven links connecting four of the telephone carriers in that area to carry national security emergency traffic for the State of California.

Each year we submit to the Executive Office of the President a national level program. The major attributes of the programs submitted to date have provided for augmentations to the public switched network, to make it more robust in both signaling—to which an issue has been made in the previous testimony—and transmission, by providing additional transmission links for interconnections, using both ground and satellite facilities, use of industry and government, especially National Guard and Reserve assets, to restore disrupted transmissions, and the equipment and the procedures to use and restrict to NSEP the additional routes, plus routes not normally used in the network.

In conclusion, let me say that, while there is always the possibility of local disruptions and after the Hinsdale disaster, if you will, one would be a Pollyanna to say there are no problems, I believe that the Nation's telecommunications networks are diverse, robust, redundant, and the qualities that make a network as a whole very resilient.

With the advice and the assistance of the NSTAC, we have created a number of programs and plans responsive to non-wartime emergencies and disasters, as well as wartime requirements, which enhance the resilience of the network. Furthermore, the NCS is currently working on new initiatives which will further ensure that the Nation's telecommunications resources will be available during emergencies such as the telecommunications networks evolve and new technologies are developed.

We have received a great deal of support from the Executive Office of the President in our activities. While I believe we are in a reasonable condition, we are in a never-ending job, because the network is in a rapid state of change and it is clearly significant that local disruptions are possible and we need the continuing support of both your activities and of the Executive Office of the President.

This concludes my prepared statement and I am prepared to answer any questions.

Chairman GLENN. Thank you very much, Mr. Morriss.

We have seen worldwide terrorism do things that we never would have dreamed possible a few years ago, including people willing to accomplish or to bring to the fore their view of things even at the sacrifice of their own lives. This has been repeated over and over again. We have been fortunate in this country that we have not had such terrorist attacks here, of which to speak.

Yours and Mr. Norman's testimony take a little more optimistic view of this than perhaps some other people. Some of the testimony and the work done before this hearing indicate a growing number of people view the situation with considerable alarm. Those critics point to the centralized nature of much of our communications, the fact that it is tending more and more in that direction, we are becoming more and more vulnerable. For example, there was testimony just a few moments ago that a dozen or so well-placed hand grenades could knock out much of the communications system in this country.

Now, granted, that would mean 12 people, say, getting access to the heart of some of our communications hubs or centralized nodes at the same time, but I do not think we can rule that out. There is a possibility that someone might try that.

I think your concerns, both of you, about electromagnetic pulse and network survivability, in general and so on, are good comments. I do not disagree with you, but I think what we are addressing here is not so much electromagnetic pulse and all-out nuclear war, as it is micro acts. Not the macro acts of destruction, but the micro acts that might bring us down short of general destruction.

Do you feel that NSTAC is addressing those concerns, as well as the big concerns of all-out war, Mr. Norman?

Mr. NORMAN. Yes, I do. We have several active task forces that are addressing such subjects. We certainly do not intend to put our heads in the sand on the issues that you are bringing up, and certainly look forward to this committee' report being issues so that we could look at it and look at the investigations that they have gone into.

At the present time, we do not share the degree of concern that they stated this morning.

Chairman **Glenn**. In your view, how much does NSTAC just advise and how much does it order, or how much should it order? We see certain vulnerabilities coming up here. Now, it is one thing to give advice, it is another thing, as I indicated to one of the other witnesses a few minutes ago, to see a frailty in the system and have to order someone to make an extra $10 million expenditures in a private business by government dictate. Is this something we are coming more and more to, or is this something that we can leave for private industry to take care of?

Mr. **Norman**. To date, the process of NSTAC advising the government in areas of concern seems to have worked very effectively. The establishment of the NCC, for example, was the first example of us working together and it has worked very well.

Each of the industries represented on NSTAC work in a competitive environment. My experience has been at the local exchange level, and we have a history of building a network that essentially works 24 hours a day, 7 days a week, that has built-in redundancies. It has not been my experience to date that new technology is making that less redundant. In fact, technology advances in the testing capabilities in particular make the detection of troubles and restoration of our network even faster than it was in the old days.

To use Mr. Lieberman's early example about one fiber pair handling 8,000 simultaneous conversations, in the old days, with the copper wires, a cable cut of that magnitude would require several hours of restoration activity, whereas the restoration of one fiber, even though many simultaneous circuits were cut off, is restored relatively fast. So, along with new technology has come some advances in detection, testing and restoration as well.

Chairman **Glenn**. Mr. Morriss, I know we have redundancy, you testified to that, but do you not feel that with the centralization we are becoming more vulnerable to something like a terrorist attack? In an EMP environment, we all know that is a big, all-out situation, we are going to have lots of problems, not just communications, but there are going to be a lot of other ones along with it. It seems to me that the specialized, the micro attack, if you will, on a few points can be almost as devastating to a communications industry. Do you feel we are going in that direction, and, if so, how do we prevent becoming even more vulnerable?

Mr. **Morriss**. I do not want to sound complacent, because I am not complacent. It is my job 24 hours a day to try and deal with the problems, and certainly the policy decisions that we have made in the past to reduce regulation and increase competition, which I happen to believe were the right decisions, but they make my job somewhere between difficult and impossible, so I understand that situation very well, and I do not, as I was misquoted in a recent article in Fortune, yearn for the good old days, but I did make the comment to them that it does make the job one heck of a lot easier when you have got to deal with a very fragmented and competitive industry.

I do not want to sound complacent, but I think there are some things that have been said that I want to go back to. It is a losing strategy to pitch yourself against the views that have been expressed by the Academy, but I think the statement that a few hand grenades is a vastly overstated statement.

First, the number of points that we are talking about exceeds the numbers that have been implied in the record, and they are for only one carrier out of the three. Second, that carrier is in the process, both partly at his own initiative and with negotiating the contract with them, to make their signaling from an NSEP point of view, not for the whole public, as survivable as the rest of his network. You would make it for the whole public, if you thought you could afford it, but it is an economic issue here.

So, I think that the statements, as I say, some of the statements have been I believe overstated. The consequences of communications failures on our society in general have gotten greater and greater and greater, and that, it seems to me, is a very major cause for alarm by all of us, but I don't think from a national security point of view that we have gotten into a worse situation. It is harder to deal with a fragmented industry, but if you look at the fact that in the National Coordinating Center, the industry has brought their people there at their expense, and we work very closely together and I am satisfied that we can fix these problems.

On the signaling thing, it was first brought to my attention by the carrier that had the problem, in the sense that we contracted with AT&T/Bell Labs to look at the vulnerabilities and they identified them. They were one of the first people that identified it and they identified it to us. They have been very open, the entire industry, in their conversations with us individually. They made us agree that we will not pass the information on to others who may be competitors of theirs and that is a difficulty.

I have found the industry very open, we have found problems and we can fix them and I am satisfied that we will continue to find them and we will fix them.

Chairman GLENN. My time is up. Senator Lieberman.

Senator LIEBERMAN. Thank you, Mr. Chairman.

You went right to the heart of what was in my mind as I was listening to the two of you. You have given us a picture that is quite different from what we heard for the rest of the morning.

Do I conclude correctly that neither of you thinks that our telecommunications systems are more vulnerable today to terrorist attack then they were 10 years ago?

Mr. MORRISS. I believe that, even though my former boss said just the reverse of that and he will take me out to the woodshed later on, because I used to work for General Paschall, there are more switches in the long-haul transmission system in this country today than at any time in history, I will make that as a flat statement. There are more routes over the Rocky Mountains, which is one place we always used to look for choke points, than at any time in history. There is more cable and satellite across the Atlantic Ocean than at any time in history.

Switches are getting bigger, cables are getting so they carry more traffic, so that when you cut one of them, a lot more people are affected and it gets an awful lot more publicity and that is not a slam at the press at all. It affects a lot more people, so it gets national attention, so you see those things happening.

We had a fire in downtown New York 10 or 12 years ago—time flies—and a lot of service was lost up there for a substantial length of time, although the industry has got an amazing record for restoring things. But there were seven switches in that building, and I would submit to you that one switch seven times larger or faster would not have been any more at risk than the seven switches that the building housed anyway.

There has always been a concentration, because of the price of real estate and facilities, maintenance guards, maintenance overhead expenses of facilities, and we are certainly getting more concentrated, but we are also getting more carriers and more diversity.

You mentioned cellular or radio, I think. It is a new way to bypass, if you will, parts of the local system. I used to say there is nothing I could do for the man who wants 911 if his end-office is destroyed, but now, in a very limited capacity sense, the cellular phone does allow that kind of thing to happen.

Senator LIEBERMAN. I take it, Mr. Morriss, that your answer embraces the reality of terrorism in the world today. In other words, when you say that we are no more vulnerable than we were 10 years ago, are you including those considerations?

Mr. MORRISS. Well, I think in some ways the threat is greater today than it used to be. We did not used to worry terrorists' incidents in this country. We worried about floods, hurricanes, tornados, which have some of the—pardon the expression, we worry about the man with the backhoe, because the cable that was cut in New Jersey was done, always on Friday afternoon, by a backhoe operator. [Laughter]

But terrorism certainly is new to this country and we have been blessed in the past.

Senator LIEBERMAN. So, even allowing for that reality and that greater threat, you feel that we are well defended in that sense?

Mr. MORRISS. I do not want to sound complacent, but within reasonable economic expenditures or within reasonable regulatory actions on the industry, yes, I think we are at a reasonable balance point.

Senator LIEBERMAN. Let me ask you another question. Why was there no Federal Government involvement in the Hinsdale episode, helping the State react to it?

Mr. MORRISS. Well, I do not know what we would have done to have helped the State. I do not know what the State could have done.

I used to go down to the National Coordinating Center after there had been a flood or a tornado and ask—they just might ask for help, and after a couple of times they did not ask for help, I said why does anybody not want help, I asked one of the carriers and he said, "Do you know how to dig holes and put up poles?" and I said no, I don't, and he said, "We have our priorities, will you please stand aside?"

Senator LIEBERMAN. So is that the key point, in other words, that presumably the people on the scene in Illinois had some sense of priorities that would have been conveyed to you that related to national security, national preparedness?

Mr. MORRIS. We have a restoration priority system which we operate in the name of FCC. In that particular case, there was an FAA man who went on the scene immediately and worked with the local carrier, not with the State because the State was the same way the Federal Government is, it cannot restore communications, except in a very limited way, but worked with the local telephone company, recognizing that he had a priority for restoration of his circuits and it happened.

We did go through and find for the Veterans' Administration, which had a number of circuits running through there into a large data bank in which they kept medical records and their burial records, in which their circuits had been lost in the process of transferring that capability from the government managed operation to an industry managed one, to identify the circuits and get those identified to industry, and industry turned to and gave those a priority treatment in their restoral actions.

Senator LIEBERMAN. Mr. Norman, did you want to answer one of those questions?

Mr. NORMAN. Yes, sir, our people at the National Coordinating Center were aware almost immediately of the Hinsdale fire and were available for assistance in coordinating the effort, if need be, but the local people and local companies involved moved almost immediately to restore the NSEP circuits, so there was no need to get involved or attempt to override anyone in the local area.

Mr. MORRISS. If I might comment on that——

Senator LIEBERMAN. Yes, sir.

Mr. MORRISS [continuing]. It is my understanding, for example, that one switch was on its way from one of the vendors into that area almost immediately. The switch was being diverted from somebody else by industry agreement, working it among the customers and industry. If that had not been the case and the switch had been needed, I certainly would have been on the phone, and my boss, jawboning somebody to make a switch available.

Senator LIEBERMAN. So, can I conclude that neither one of you shares Mr. McDonald's conclusion that there is a need for more planning at the Federal Government level to deal with a telecommunications emergency that might be caused by a terrorist attack?

Mr. NORMAN. Yes, I do not share that opinion. Certainly, the threat of terrorism is greater than ever before, but I do not see a deterioration in our capability to respond to a crisis, because of either competition or technology. In fact, I see the opposite.

Mr. MORRISS. It is a matter of degree. I think we are doing a lot of those things already and I think we have to continue to do them.

Senator LIEBERMAN. Thank you, Senator.

Chairman GLENN. This idea where we are moving more and more to computer controlled systems, does the business of hackers getting involved bother you, and are we doing anything in that area?

Mr. MORRISS. We are not and it does not bother me with respect to the telecommunications industry, for the following reason: You used the term "hacker," and I want to distinguish between a hacker and a disgruntled employee of the firm which has access to other things, because I think it is a great distinction to be made there.

Chairman GLENN. Address both of them.

Mr. MORRISS. Well, let me address first the hacker and then the other one. The hacker problem says to get in and do something malicious inside the computer, and I look on an electronic switch as a computer. You have to be able to put a program in there that the computer then operates, that is how the virus takes effect. You cannot just, using a computer to transmit information, which is what goes on in a telephone switch, actually infect it or disrupt it from the outside. You can disrupt the computers that are tied onto the network, and that is what has been done in the past.

ARPANET did not get infected, using the example I believe by somebody earlier, by a hacker. It was used by a hacker to infect computers that were tied into the network. So, in the hacker sense you have got to be able to get into the operating software of the computer and operate it, and a hacker generally cannot do that.

A disgruntled employee can do that, and that it seems to me is a potential liability. Now, it is an easier thing to try and deal with, because a lot of employees are looking at other employees. No software goes out to the field without being very thoroughly tested by a lot of different people. Having said that, software gets to the field and it has errors in it, I recognize that.

Chairman GLENN. Just one last question. Is NSTAC going to be continued by the new administration, as far as we know?

Mr. NORMAN. We certainly hope so.

Chairman GLENN. There has not been an indication or a decision yet?

Mr. MORRISS. There is every reason to believe that it would be. It operates under a sunset clause and would in theory operate unless somebody took a positive adverse action until this coming September.

Chairman GLENN. It has been reauthorized, what, twice or three times? Twice, is that correct?

Mr. MORRISS. Yes.

Chairman GLENN. Okay. As far as we know—well, we do not know what the current administration's view is then?

Mr. MORRISS. We have every reason to believe that it will be continued.

Chairman GLENN. It will be continued?

Mr. MORRISS. Yes.

Chairman GLENN. Okay. Thank you.

Do you have anything else?

Senator LIEBERMAN. Just one more question, Mr. Chairman.

NCS, as I understand it, focuses "on national security emergency preparedness." To what extent will restoration of telecommunications services to meet NSEP needs also restore telecommunications services that businesses and residences depend on?

Mr. MORRIS. That is hard for me to generalize on, because certainly some of the things that we do with the industry does help, but we are not trying to point ourselves to solving that problem. I have to agree that that is not in our bailiwick.

Some of the things, such as the restoration priority system we have, can help industry where it has a responsibility for national security emergency preparedness. It could help, for example, coordination in restoring the power grid communications, because that is mandatory to bring the power grid back up in some cases, so those could be given under that system a priority, and it would be applied. As I say, it was applied in the Hinsdale situation. But just general business, no, we are not really attacking that problem.

Senator LIEBERMAN. We have heard testimony today about the tremendous financial dislocation that could result from a terrorist attack on the telecommunications system. Is anybody at the Federal Government worrying about that part of it?

Mr. MORRISS. Not to my knowledge.

Senator LIEBERMAN. Do you think there should be?

Mr. MORRISS. No, for the following reason: To get in and worry about it says you are going to do something which I believe in general industry can do for itself if it is willing to pay the price, and it costs money. I am told, for example, after the October, whatever happened on Wall Street a year-plus ago, where people could not reach their brokers and so forth, a lot of the industry itself went into a number of backups and expanding their telecommunications facilities. A microwave facility was put in, for example, on the Exchange floor in a backup and a bypass to the other facilities that they have. Those things are all available as services if one is prepared to pay for them.

The question that one always has is how much insurance does industry feel willing to carry, and my own belief is that is a decision that you leave to industry.

Mr. NORMAN. I might add that the network plan is not trending towards one large digital switch and one large fiber-optic cable. It is not unlike the development of the national highway system. It is developing one leg at a time and most major metropolitan areas, a network of switches and fiber-optic cables are being built to ring and criss-cross major metropolitan areas. So, the trend is for a more robust architecture as it grows.

Chairman GLENN. How many terrorist threats did your industry receive last year?

Mr. MORRISS. I do not really know of any, because I do not think there were any terrorist incidents that I am aware of against the industry last year.

Chairman GLENN. If the CIA develops a source that says there is a threat to your industry in a certain area, or the FBI comes up with some information, what is the procedure?

Mr. MORRISS. There would be two procedures for that. I am thinking primarily of the FBI, which is the organization with which we have worked. They would first make the information available to the National Coordinating Center, which has a way to go back into each of the companies and the carriers from there, to alert them. They would also try and go back through their local FBI offices to the people that are in the area of that FBI office, and that part of it is now being sorted out, I think, because there is a lot of communication that has to take place within the FBI as to who, if you have the warning of an incident in this area, who do you talk with and what company, and that is the process with the FBI and ourselves and the industry representatives.

Chairman GLENN. You do not know whether there were any such warnings put out this past year?

Mr. MORRISS. I do not know of any, sir.

Chairman GLENN. Do you know, Mr. Norman?

Mr. NORMAN. No, sir.

Chairman GLENN. That is something we might want to look into and get some information on. I am not aware of any, either, but the procedure would be that they would go through you and then to the NCC and then to the companies?

Mr. MORRISS. They would go two ways. They would go through the National Coordinating Center, into the companies, and we would provide that for the top-down, if you will, and the FBI would go through their regional offices back into the facilities that are in those regions.

We have to rely on the local, either the industry itself, its own guard forces or the local law enforcement people to do this. There is no way the Federal Government can, of course, provide the number of guards for the FBI's ability to alert and maybe they can provide some local assistance, and it is extremely valuable.

Chairman GLENN. You are not saying there were none; you are just not aware of any?

Mr. MORRISS. That is correct, I am not aware of any.

Chairman GLENN. I will not take the other side and argue that, but your testimony, that you feel a threat is very low, I think that would be a key element, knowing how many threats we had last year and what happened to them, before you could make that judgment.

Mr. MORRISS. I am not making a judgment, sir, that the threat is low. I think that we have taken reasonable steps to make the system resilient and reasonable steps to respond to the actions, but I would not say that I think the threat is low. I just do not know of any warnings last year. We have been blessed by not having terrorist action in this country. I do not know why.

Chairman GLENN. And may that continue?

Mr. MORRISS. Yes, sir.

Mr. NORMAN. Amen.

Chairman GLENN. Thank you. We will have another hearing tomorrow morning at 9:30, in which we will go into basically the energy areas, electricity, oil and gas supplies in the country, and how vulnerable they may be.

The Committee will stand in recess until 9:30 tomorrow morning. Thank you all.

[Whereupon, at 12:27 p.m., the Committee recessed, to reconvene on Wednesday, February 8, 1989, at 9:38 a.m.]

VULNERABILITY OF TELECOMMUNICATIONS AND ENERGY RESOURCES TO TERRORISM

WEDNESDAY, FEBRUARY 8, 1989

U.S. Senate,
Committee on Governmental Affairs,
Washington, DC.

The Committee met, pursuant to notice, at 9:38 a.m., in room SD-342, Dirksen Senate Office Building, Hon. John Glenn (Chairman of the Committee), presiding.

Present: Senators Glenn and Lieberman.

OPENING STATEMENT OF CHAIRMAN GLENN

Chairman Glenn. The hearings will be in order.

This morning, the Governmental Affairs Committee will conclude 2 days of hearings to consider the vulnerability of our telecommunications and energy resources to terrorism, and the sufficiency—and this is the main thrust of it—of Government organization and activity to reduce this threat and vulnerability, and how we are organized to deal with it if anything like this does occur.

Today, our focus will be on the Nation's energy infrastructure, including the electrical transmission and generation system, and the pipelines which move natural gas and other petroleum products. In Europe, Central America and the Middle East, terrorist activity has increasingly targeted such facilities. These systems include tens of thousands of miles of pipes, wires and facilities. Even using military resources, it is not possible nor desirable to physically protect every portion of the network from vandalism or sabotage. However, it is important to understand what portions of these networks are vital to the provision of necessary services; how well protected or redundant these facilities are; and whether they could be readily replaced in the event of damage.

The U.S. energy infrastructure has generally proven to be resilient and reliable. The fundamental issue is whether the system can respond to a successful multisite terrorist attack. There is a real controversy over the degree of vulnerability in the system. Today's hearing may be very important in giving the Congress a better understanding of how vulnerable we really are.

Again, today we will begin by hearing an actual reminder of how serious a problem loss of services can be to a local populace—in this case, loss of electric power due to an accidental fire. Last fall, the city of Seattle lost power in its downtown area for 4 days over a holiday weekend. In a less hospitable climate, or at a different time of the year, such an event, or a larger outage, might present very serious difficulties for our citizens. This is just one community and what happens when there is an event like this.

This morning, we will be focusing on the adequacy of the Government presence in this area, which appears less well developed than in the telecommunications area. Important collaboration between industry and the Department of Energy is under way, and the impact of this collaboration needs to be assessed. We need to ensure that the level of cooperation we have reached today continues into the next administration. We may need to improve the degree of attention currently being given to the potential impact of terrorist activity.

I would add that we are concerned about the impact of technological developments on communications nodes, as they are called, or centers of communication or centers of transmission of a particular energy. Those central points, if destroyed, could possibly bring down a system for a lengthy period of time. And, if done on half a dozen sites at the same time, it could well disrupt major parts of our whole United States. That does not overstate it. It is obviously an economic concern as well as a national security concern.

Responsibility for dealing with this has been spread around somewhat. For example, the FBI role has changed somewhat and is something we may have to go into at a later date. The FBI, which is the lead Federal agency responsible for investigating domestic terrorism, has been tasked under Executive Order 12656 with the duty to assist heads of Federal departments and agencies, State and local governments, and the private sector in the development of plans to physically protect essential resources and facilities. Maybe we can learn today from DOE whether this new FBI responsibility will reduce or change DOE's former primary role in this area. The responsibility of this committee is to oversee these organizational aspects of Government and to make sure that they are adequate.

Along that same line, the Honorable George Woloshin, Associate Director of National Preparedness at FEMA, Federal Emergency Management Agency, gave testimony last fall before a Subcommittee of the Judiciary Committee. In his testimony, he said:

> As a related matter, we would like to call your attention to a letter the Director sent to the Attorney General July 26, 1988, calling his attention to the shift in physical security responsibilities contained in the revised Executive Order 11490, and recommending the Department of Justice chair an inter-agency group with planning oversight responsibility for the asset protection program. DOJ, the Department of Justice, has subsequently concurred with this recommendation and delegated the responsibility to the FBI.

So that is another area that we may have to get into.

We are pleased to have representatives of the electric industry here. Unfortunately, representatives of the oil and natural gas pipelines who were invited to participate in these hearings have declined to do so. They felt that they did not want to go public with some of their testimony, that they will tell all, in effect, if we want them to do so, in private session, and we may want to do that later on. We did not want to close the session this morning when we were trying to lay out the whole problem in a much more general way. But, I appreciate their concerns. I do not agree with their decision not to testify, because I had given quite adequate assurance that if we got to anything they felt was of a really classified nature or really was pinpointing specific spots that might invite terrorist attack by public discussion of those points, we would close the hearing, classify the documents involved, and would protect it in that way.

The last thing I am trying to accomplish with these hearings is to lay out any blueprint for anyone who wishes us ill. But, at the same time, we have a responsibility to make certain that our Government organization, our Government planning, is adequate to deal with this as much as we possibly can deal with it.

We have seen terrorist acts wreak havoc in other parts of the world. We want to make sure that we prevent that as much as we can or that we are prepared to deal with it when it occurs here. The purpose of these hearings is not to try and lay out a blueprint for anybody. Our purpose is to see what the Government is doing in its organization to make sure that these things do not happen, or how we deal with them if they do happen.

As I indicated yesterday, and as I would remind our friends in the oil and natural gas pipeline who declined to testify today, this is not a brand new subject. I put into the record yesterday a list of dozens of hearings or writings or reports that have dealt with different parts of this whole problem. So, this is not something that is brand new and is going to invite terrorism. Quite the opposite. We have had a lot of study of this through the years, most of it since 1982. There were a couple of reports before that. As I recall, most of them were undertaken since 1982. We may need to have some private sessions where we get information from the oil and natural gas pipeline people.

In private discussions, both of these associations acknowledged the fundamental vulnerability of certain areas in their networks to multisite terrorism. So I hope they will redouble their efforts to cooperate with the Department of Energy, with the FBI and anyone else involved, to ensure that access to their products are not denied to the Nation.

Before introducing the witnesses for today's hearing, I want to renew the instructions I gave to all the witnesses yesterday: If you believe the answer to any question is unusually sensitive and should not be made in public, please feel free to indicate this. No specific location should be mentioned to address the vulnerability issue. We are addressing a couple of specifics just to show what happened with a particular city when something like this occurs, but I am talking about a specific location of any utility or facility that would be particularly vulnerable. I do not want any of those brought out in public testimony. No specific location should be mentioned to address the vulnerability issue.

Having said this, I wish to emphasize once again that our focus in this hearing is the role of Government in ensuring that the national security component of energy production and planning is addressed. We want to be sure the Government agencies charged with responsibilities in this area are doing their job, good coordination is being achieved, and cooperation between Government and industry in this area is maintained. These issues can and should be dealt with in open, public hearings. The American people have a right to know what vulnerabilities they face in regard to potentially life-threatening disruptions in energy supply and what their Government is doing about it.

I would like to include Senator Sasser's statement in the record. Without objection, it will be included in the record in its entirety. He was not able to be here this morning. He is appearing before another Committee also this morning.

[The prepared statement of Senator Sasser follows:]

Opening Statement of Senator Sasser

Mr. Chairman, 2 months ago all of America was riveted by the tragedy of Pan Am flight 103. More than 250 innocent people were killed in a deliberate and carefully planned act of sabotage. As we all know this was not the first time such a savage act has been directed against American citizens. Unfortunately, the tragedy of Pan Am flight 103 serves as a stark reminder that despite America's great might, violent individuals and groups can inflict death and destruction with a minimal amount of resources and effort.

Nonetheless, while past history has shown that terrorists and other anarchical groups prefer to attack their perceived enemies through high profile means such as assassinations, hijackings and bombings, there now seems to be the realization that greater overall damage can be inflicted on a nation or government by attacking nonhuman targets.

Today, America and many other nations are to varying degrees dependent on sophisticated distribution networks to provide needed communication and energy services. In the United States, these intricate hi-tech networks efficiently channel the resources that power cities, fuel industries and keep Americans in touch with one another. By utilizing the latest means in transfer technology and automation, municipalities and corporations are able to manage these networks so that individuals, businesses, and government offices, can carry out their daily activities.

As testimony presented for the hearings indicate, in the past, there have been isolated incidents in which an accident or natual disaster has disrupted the operation of a certain network, resulting in serious consequences for the communities and businesses affected. Who can forget the scenes of looting and vandalism during the famous New York City blackout. More so, these examples provide an adequate indication of the potential consequences of a planned mass disruption of crucial networks located in the United States.

Today, many experts in the government and industry acknowledge that terrorist groups are beginning to recognize the vulnerabilities of these highly developed, technology dependent networks. They also recognize our high degree of dependancy on these networks. Some countries, including vital allies, have already experienced attacks on these networks. And it gives me a chilling feeling when I read testimony stating that "a few well-placed hand grenades would crash the entire AT&T network."

While the United States has not experienced such an attack, it seems that the reason is not because our facilitis are inaccessible or invulnerable to attack. On the contrary, as expert testimony has indicated, U.S. systems, particularly those in the energy and telecommunications field, are very vulnerable and inviting targets. Technological advances and economic competition have created highly concentrated systems that use fewer routes and fewer switching stations, and lack media diversity.

Nonetheless, while there is debate over the degree of danger U.S. facilities face due to terrorism, of more immediate concern is how to control the damage of a disruption caused by natural disasters and accidents. All of the major disruptions that have happened in the United States so far have been the result of non-deliberate or natural acts.

Therefore, it is my sincere hope that these hearings can help to enhance the dialogue and preventative planning that has been taking place between the Federal Government, municipalities, industry and any other involved parties. In case of an emergency, whether on a national or a local scale, or whether as a result of sabotage or an accident, there has to be viable and operational contingencies that will allow vital services to continue to operate uninterrupted.

We can not allow the evolution of a situation where in the event of a disruption citizens are without 911 service, hospital are without electricity, and emergency vehicles are without fuel. For it these types of situations are somehow allowed to transpire, tens of thousands of Americans will be victimized and surely our Nation's social and economic well being as well as our national security will be compromised.

Chairman GLENN. Our first witness this morning is Dr. Robert K. Mullen, independent consultant. He will be followed by Mr. Randall Hardy, superintendent of Seattle City Light, and Mr. Charles H. White, division staff executive, Power Equipment Division of the National Electrical Manufacturers Association.

Panel 1, then following, will consist of Mr. Michehl Gent, President of North American Electric Reliability Council; and Mr. David Hinman, manager, Corporate Security, Alabama Power Company. Panel 2 will be Mr. Edward V. Badolato, Deputy Assistant Secretary for Energy Emergencies of the Department of Energy.

Dr. Mullen, if you would come up to the table, please, we would appreciate your testimony, either in its entirety or an abridged version. In either event, the entire statement will be included in the record as delivered.

TESTIMONY OF ROBERT K. MULLEN, Ph.D., INDEPENDENT CONSULTANT [1]

Dr. MULLEN. Mr. Chairman, I am pleased to have the opportunity this morning to share with you my perceptions of subnational threats to U.S. energy systems. These perceptions have been formed from my assessments of subnational energy assets sabotage incidents over the past three decades.

My scope of interest in these regards is entirely subnational; that is to say, I do not concern myself with the potential or actual threats to these systems from national adversaries, such as the special forces elements associated with the military of any nation. My focus is on those adversaries termed "terrorists," "insurgents," "criminals," "employees," and others not possessing the qualities of a national adversary.

Before I get to the sabotage threat in the United States, it may be useful for me to outline, at least superficially, subnational sabotage activities outside the United States for a couple of reasons: First, because most of it is qualitatively and quantitatively different from what has and is occurring here; and, second, there is concern that this could change.

In Europe, separatists, anti-NATO militants, environmental extremists and others have and continue to sabotage energy assets there. Individual targets such as the refinery in Tarragona, Spain, have suffered millions in damage in lost production and damage to plant and equipment from an individual act of sophisticated sabotage that occurred in 1987.

NATO pipelines were the object of a campaign of sabotage by terrorists in Belgium in 1984 to 1985, and the NATO headquarters in France for wartime petroleum distribution in much of Europe, was also bombed by the same group.

In 1986, sabotage against power pylons in West Germany was exceeded in frequency only in El Salvador. About 150 pylons were bombed in that year. Also in that country, the infrastructure supporting the nuclear power industry has been the object of sabotage that is remarkable for its depth. Construction firms—some bombed or fire bombed 30 to 40 times—trucking companies, railroads, including track and rolling stock, security firms, architectural and engineering firms, consulting firms, banks and other financial institutions with ties to the nuclear power industry, nuclear equipment manufacturers, scientific and technical institutions, and assets of all kinds owned by utilities that generate power by nuclear means, are among those who have been attacked by terrorists and antinuclear extremists in West Germany.

---

[1] See p. 239 for Dr. Mullen's prepared statement.

Assassinations of professional personnel and executives associated with the nuclear power industry have occurred in France, Spain and West Germany. These have been carried out by Direct Action, the ETA and the Red Army Faction, respectively.

Elsewhere, in pre-industrial nations for the most part, sabotage against energy facilities is carried out by insurgents. Facility isolation, the lack of effective grid structures—in the case of electrical distribution systems—and the abilities of the adversaries in some cases to deny areas to Government forces, even temporarily, contributes to the effectiveness of their sabotage.

In Colombia, for example, these factors contribute to the ease and frequency with which the Cano Limon-Covenas crude oil pipeline is being sabotaged. In the first half of 1988, the National Liberation Army caused Colombia several millions in lost crude oil, repairs, and lost export revenue.

Of course, in El Salvador, the FMLN guerrillas take advantage of those factors to keep large segments of the nation in darkness and without drinking water for extended periods.

In Mozambique, the Mozambique National Resistance has taken advantage of these factors to bomb over 1,400 power pylons on the Cabora Bassa power line to South Africa. Nine hundred of these have been bombed since April of last year.

In Surinam, the Ronnie Brunswicjk followers could bring that nation's economy to its knees with half a dozen or so explosive charges applied to the power supplies at the bauxite mine and a bauxite ore refinery, and then denying the areas to repair crews. Bauxite is Surinam's principal source of foreign exchange.

In the United States, the most common acts of energy assets sabotage are gas station bombings and arson, and shooting at powerline insulators. This, in part, contributes to the numbers of energy sabotage incidents noted in the tables that accompany my more detailed statement submitted previously. One sees few accounts for these and similar incidents outside the United States, and this can distort somewhat the impression one gets by comparing only the numbers within the United States and other nations.

Having said that, there are in the data notable incidents of energy assets sabotage in the United States. In 1980, 50 H-frame structures supporting 115-kilovolt powerlines in Colorado were sawn by persons unknown. In 1981, a utility in Florida suffered some $3 million in damage from bombings and rifle fire directed at power substations during a labor dispute. In 1984 to 1985, labor difficulties at West Virginia and Kentucky coal mines led to a number of powerline bombings and power substation sabotage. Coal mine equipment was repeatedly bombed, and shootings resulted in several woundings and one death.

In 1986, several individuals grounded three 500-kilovolt power lines leading from a power station.

In 1987 to 1988, there was an intense campaign of sabotage against energy assets belonging to or supplying coal mines in Wyoming and Montana. A dozen or so power poles were bombed, as were several power substations. Damage estimates for the period approached $2 million. These activities occurred during labor disputes and ceased when a coal company and the utility offered a $250,000 reward for information leading to the arrest of any of the perpetrators.

Insofar as energy system sabotage trends in the United States are concerned, there are no indicators of which I am aware that would suggest to me the threat to energy assets here is substantially different from what the historical record indicates. Subnational threats to energy systems in the United States are in many ways different from those in other nations, industrial and pre-industrial.

The possible relevance of the realities of significant sabotage in Europe to the threat of such in the United States is weak. The record of energy assets sabotage in the United States does not reflect the occurrences of incidents motivated by the concerns of European terrorists.

Further, there is little or nothing in this record approaching the level of violence, the intensities of sabotage campaigns, or the sophistication of sabotage committed by terrorists in Europe. What parallels there are reflect the unsophisticated power pylon, power substation and service station bombings that occur in Europe and the United States.

Targets, for the most part, are chosen for their relative isolation, accessibility, and simplicity, rather than for their significance to the operation of any particular system.

This is, for the most part, true in pre-industrial nations as well. The difference there, however, is that the sabotage is frequently more severe in consequence terms as there is less flexibility in the energy systems than in industrial nations, as the United States Furthermore, when key energy assets are targeted, they are often attacked by large numbers of people supported by mortar and rocket fire.

There are no parallels in the United States Very little of what occurs with respect to energy sabotage in pre-industrial nations is comparable to what occurs in the United States What similarities do exist, such as the lack of sophistication and the opportunistic nature of most sabotage acts, reinforce my perspectives concerning trends in the United States, which is to say that I see no indicators that sabotage trends here will diverge in any significant way from what the historical record indicates.

This concludes my statement. I would be pleased to respond to questions.

Chairman GLENN. Thank you very much, Dr. Mullen.

Some of the things that you mention are incidents, I guess we would call them, by smaller groups to make a particular point in a particular area. Have there been any terrorist acts in Europe, or elsewhere around the world, that were planned on a more national basis? In other words, planned to knock out major portions of energy supply or communications over a more lengthy period of time?

Dr. MULLEN. Not on a systemwide basis that I can discern. There have been events in Europe, a half a dozen or so since 1981 or 1982, in which the primary distribution lines from power stations were taken down. This in some cases forced the power station to go off line or to reduce power. This is not an insignificant economic consequence to the utility. As a general rule of thumb, the value of the electricity generated by a 1,000-megawatt power station, is roughly a million dollars a day. That is lost revenue for the time it is down.

In addition to that, the utility owning the power station must purchase power from other generators on the grid, and there is also the expense of repairing damage to the facility from primary and secondary causes.

Chairman GLENN. How much of this has been caused by anti-nuclear forces? We have a lot of people around the world who just do not like anything nuclear, including nuclear electric power plants or any other kind of nuclear activity. Has there been targeting of nuclear facilities by those groups in particular?

Dr. MULLEN. Yes, there has, especially in the Federal Republic of Germany. The antinuclear movement, so far as I can determine, is a subset of a larger antitechnology movement there which is quite violent. The targeting, however, seems to be somewhat opportunistic in nature. The range of targets is wide. Nuclear fuel shipments are targeted; power reactors are demonstrated against by 20,000 to 50,000 people.

For any particular incident, the more radical elements, rather the terrorists—the RZ, the revolutionary cells, RAF—will participate in such demonstrations to the extent that they recruit individuals into their own ranks at those demonstrations. The nuclear industry and the infrastructure supporting the nuclear industry in the Federal Republic of Germany has suffered considerably from the hands of not only terrorists, but what is called in Germany the "feuerabendterroristen" or the "after-hours terrorists." People who are bank clerks, truck drivers, and whatnot, after work go out and saw down a power pylon.

Chairman GLENN. When you looked at this situation around the world, the worldwide statistics, did you form an impression that our allies in Western Europe and Japan take these terrorist threats very seriously, and that they have active programs against such activity?

Dr. MULLEN. Indeed, they do, particularly in West Germany, the nation that has perhaps suffered the most. They have gone so far as instituting a neighborhood watch program, if you will, circularizing millions of people with postcards to look out for anybody in the neighborhood you do not recognize who may be approaching a power pylon, for example. It has been fairly effective.

In 1986, there were approximately 150 such events directed against power pylons. The following year, there were 60-some, and last year there were 43, I believe.

Chairman GLENN. Well, following up to their taking it seriously and what they are doing about it, how does that compare with our organization to deal with such matters here? Can you compare their preparation and our preparation?

Dr. MULLEN. Not very well. I believe Secretary Badolato will have something to say about that.

My focus is primarily threat. When it comes to security and vulnerability, I am not an expert.

Chairman GLENN. In most foreign countries, the energy and the telecommunications infrastructure is owned by the Government or a Government-controlled corporation. Does that change the nature of it, giving them an advantage as far as security planning goes, compared to our private industry approach to these areas?

Dr. MULLEN. I do not know. I have never looked at it from that standpoint. In the Federal Republic, for example, the power industry is in private hands. In pre-industrial states, most of the power industry is in state hands. It is difficult to contrast what occurs in many pre-industrial states with what occurs and is occurring in industrial states for a number of reasons.

Electrical distribution systems, for example, in many pre-industrial states follow the roads that were built by former colonial powers to go into the interior and to extract the natural resources from that colony and export them back to the mother country. When electrical systems were built, they followed those roads, which do not interconnect. The grid situation is very weak in these countries, and it is difficult to contrast what goes on.

There are terrain problems. The Andean nations have particular difficulties in that regard.

Chairman GLENN. Thank you, Dr. Mullen.

Dr. MULLEN. My pleasure.

Chairman GLENN. We appreciate you being with us this morning.

Our next witness is Mr. Randall W. Hardy, Superintendent of Seattle City Light. He's here to give us an example of what can happen in just one community when these events occur, which was more an accident than planned sabotage.

Mr. Hardy, welcome this morning, and proceed with your testimony.

TESTIMONY OF RANDALL W. HARDY, SUPERINTENDENT, SEATTLE CITY LIGHT, SEATTLE, WA [1]

Mr. HARDY. Thank you, Mr. Chairman.

My name is Randall W. Hardy. I am the superintendent of Seattle City Light. We are the seventh largest public utility in the United States and serve the municipality of Seattle plus a portion of service territory both north and south of the city.

The incident that I will describe today was a major outage that we had surrounding Labor Day weekend last year, 1988. It was a 4½ outage. It covered roughly a 50 square block area in a portion of downtown Seattle. The whole city was not blacked out; about a third of the city was blacked out. Needless to say, however, a blackout of this duration and of this extensiveness was a major event within the city, and even to some extent nationally, given the amount of media attention that it attracted.

The immediate consequences of the event were, in retrospect, fairly predictable, but something that always seems to surprise you, given that you do not cope with these things every day. Substantial quantities of people were stranded in high-rise buildings without elevator service or sometimes other means of coping with this event. Substantial concentrations of low-income and elderly people, particularly in the specific portion of downtown Seattle where there is a high incidence of hotels that served low-income and elderly, and that was a particular problem that necessitated the procurement of emergency generators on very short notice to try to keep at least minimal electric service to those facilities.

---

[1] See p. 258 for Mr. Hardy's prepared statement.

Obviously, there were no traffic lights or electronic traffic signals in the entire blacked out area. Food spoilage, most of the restaurants had to, in fact, throw out all of their food within 12 hours of the outage occurring because refrigeration simply was not available.

Finally, the predictable security problems in the blacked out area. Any time the lights are out in a 50 square block area in any major city, you worry about looting; you worry about other kinds of local security problems that may arise.

In retrospect, we made out, I think, much more fortunately than might otherwise have been the case. The potential for things to have been worse was clearly there, but several factors combined—while this was a unique outage, certainly it could have been a lot worse.

The factors that helped us were, first of all, we had two transformers in the vault where the fire occurred. Neither of those transformers ruptured. Had there been a rupture, there very likely would have been an explosion that could and probably would have killed some people in the surrounding area. The two transformers also were PCB-contaminated, not excessively so but enough that we probably would have had to evacuate the surrounding area for several square blocks. With the transformers remaining intact, even though the fire was pretty intense, we avoided both the PCB problem and any effects of an actual explosion.

The weather was hot. It was over 90 degrees. While that made for some rather onerous working conditions, I would have much preferred to deal with that kind of an event rather than weather like we have today or today out in Seattle, where the temperature is below freezing and stays below freezing for most of the past few weeks. That would have presented us with people freezing in the dark and other kinds of images, as well as realities, that would have made our task much more difficult.

Other things that worked well, not environmental factors so much, the city responded well. The citizens responded with a unique degree of tolerance and good humor to this event. I do not know if that is unique to Seattle. Certainly, we have had that response in other areas with other problems. That may or may not be the case with other cities in the United States. But that made our job enormously easier than it might otherwise have been.

We had excellent cooperation. We handled this exclusively at the local level. We did not have to involve State or Federal agencies—not that we would not have if we needed their assistance, but we were able to marshall our own resources, with particularly the local fire department and police department working with us as the electric utility to handle most of the problems that came up.

We were able to do that because the size and duration of the outage was, in fact, manageable. Had the outage been over the whole downtown area, I am not sure that would have been the case. As it was, our resources were pretty well stretched to the limit to handle this kind of an outage.

Also, we had essentially a 4½ day outage. While we got through that okay, I am not sure, had the outage continued on for another 3 or 4 days, that we would have continued to enjoy the kind of citizen tolerance that was exhibited for the actual outage in question.

I would like to just spend my last couple of minutes of my testimony, Mr. Chairman, going over some of the lessons that we learned. In retrospect, they are not too different from lessons that you learn in most disaster planning exercises, but they are important.

The first lesson that is the most critical one, I think, is the effective management of the response team that you have on scene. In point of fact, utilities are pretty well equipped, I think, to deal with some of these things because we handle outages of various durations and sizes almost every day. But getting a single point of coordination and a single point of leadership at the scene was vitally important: to resolve the inevitable disputes you had of allocating resources, to provide centralized policy direction, and to provide the visibility, both to the work force and to the general public, that someone was in charge. I spent virtually about 18 to 20 hours a day for 4½ days on site directing the operations. Not the technical operations so much, but handling the media and handling the inevitable logistical and jurisdictional questions associated with—well, was the fire department going to do this, or was the light department going to do it, or was the police department going to do it?

Second, we had daily meetings; whether they are daily or some other frequency, you need periodic meetings with all of your people there where you sit down, figure out where you are internally in restoring the power, what your game plan is going to be for the next 24 hours, clarify what your work assignments are so everybody knows what their responsibilities are and when they are going to get things done by; and, finally, someone there to make the policy calls and set the priorities, if there are conflicts, on how to do that.

We did that. It worked well. It is the same kind of thing you do in almost any disaster planning exercise, but it works in the real world as well. It is the same kind of thing, you know, with the 10 years in the Navy that I have gone through and numerous other military-type exercises. The same principles apply for this kind of activity.

The second lesson is the importance of coordination among agencies, whether they are Federal agencies or whether they are local agencies. In this case, it was local. We worked with the police department to provide security. They put on 50 extra officers patrolling the blacked out area immediately. We actually had less crime in the blacked out area than we normally do. That is because the police presence was so intense. It is also because we worked with the police department to rig temporary street lights in the downtown area. So by the second day of the outage, we had already strung street lights to the most critically affected areas in the police department's judgment. By the third day of the outage, by Friday night—the outage occurred noon on Wednesday—we had rigged temporary street lights to the entire blacked out area.

Close cooperation with the fire department. The fire department was our primary link in terms of determining the fire protection in different buildings. Also because they had to go into each building and determine what the state of fire protection was, they were key in working with the Red Cross and with us in identifying where we had concentrations of low-income, elderly, other populations that would have difficulty coping with the loss of electrical power. Then we could work particularly with the Red Cross to get resources to those particular people in need; and the city and county health department, similarly, for food spoilage, for other kinds of health conditions that were occasioned by the outage.

The third lesson is the importance of emergency response plans. In this respect, I think we were reasonably well equipped. I think electric utilities probably generally are pretty well equipped because we cope with outages on a daily basis. This is not a unique experience. The scale of this one certainly was, but we have the basic mechanism in place to handle these kinds of contingencies on a very regular basis. It is just a matter of scaling that basic structure and set of emergency response procedures up to the appropriate level. We were able to do that; it worked well.

The fourth lesson was the importance of communications. Mobile phones are worth their weight in gold in this kind of a contingency. We do our normal dispatching operations on walkie-talkie regular single side band kind of radio circuit, which works well where you have one dispatcher and then a bunch of crews that are going out. But you cannot fill up those circuits with individual calls when you have to call the engineer back in the main building and say: What about this print and where does this wire go? That is where you need a mobile phone. Or you are calling around from the site, trying to procure an emergency generator to a particular location.

Granted, there are other natural disasters—earthquakes come to mind—where they could be so extensive that your cellular phone network would be interrupted as well. But for somewhat localized disasters of this type, we found that a good supply of mobile phones was probably the single most important communications asset that we had.

The fifth lesson and probably the most important was media coordination. We had 500 media contacts in 5 days, everybody from the local stations to CNN. That was probably the biggest difference that we had from a normal outage. We tried to handle that by centralized control. I was at the scene, as I described before, almost 24 hours a day. I handled all the media at the scene, and we had our own folks on around-the-clock watch back at their main building that handled all the phone contacts from primarily national news as that occurred.

It was important that there was a single message going out as to what we were doing, where we were, what our expectations were for the next 24 hours, so that there was an image as well as the reality of competence and someone who was in control, and that the public was getting a consistent message. It also helped, particularly at the site, in that I could handle that kind of inquiry from the media and not have our technical people diverted from spending time from getting power restore because they had to handle media inquiries that inevitably diverted their attention from the task at hand. So we divided the responsibilities in a way that worked out well.

The final lesson in this whole exercise about media coordination is probably the most important. The local media, in particular, were the single most valuable communication asset we had to tell people what we needed them to do. Probably the best example of that was when we finally got to Saturday evening and were going to turn the lights back on, we were quite concerned about a power surge. Typically, your initial surge is three to four times the amount that your load eventually levels out at. We were concerned that we would overload the circuits. We were not able to bring all of our major feeder cables back at one time. We actually were only able to bring four of the six back that normally serve that area. So we put the word out primarily through the local radio and TV media for people to turn off their water heaters, to turn off their air conditioners, to turn off their home computers so that we would keep the power use down to a minimum level and avoid the surge problem.

As an example of how well that worked, our normal load in the blacked out area is 35 megawatts. We expected, given that we had locked out some loads at the start, that we would see a lot of 10 to 15 megawatts when we actually reconnected. When we first reconnected, the load was so low it did not even register. Finally, after 2 or 3 minutes, it settled out at 3 megawatts for what is normally a 35-megawatt area. That is, I think, almost exclusively because people were tuned in to what was happening; they were listening to their local media; and we were getting better communication through the local radio and TV stations than we could have achieved by any other means.

I think that is probably the most important lesson in all, and I suspect that that would be—you would see a similar dynamic in almost any natural disaster. The media are your allies in this kind of a situation, as long as you are candid, as long as you are up front with them, and you make them part of the team. That is the way it worked for us, at least until we got the lights back on, and then we had the predictable blame assignment stage of this thing. But you deal with those problems as they come. But in terms of getting the power restored, they were extremely helpful.

I would just say in the way of general conclusions, it could have been worse. Certainly, it demonstrated the pervasiveness of electricity and the importance of that to our society and to Seattle in particular. We coped pretty well. Our resources were stretched. I think we could have coped with a larger outage, but that would have taken a larger scale and response and probably had to involve other agencies. Our people performed magnificently, but it is not an experience I would care to repeat.

Thank you very much, Senator.

Chairman **Glenn**. Thank you.

Yours was a fairly localized situation. Were there any hospitals or similar institutions in the middle of the blacked-out area?

Mr. HARDY. No. We were very fortunate there were no medical facilities

Chairman GLENN. Did your planning include calling in the National Guard, or anything like that, had there been a bigger area affected?

Mr. HARDY. If we would have gotten to that stage, I am sure we would have considered that. Our normal disaster planning for the city is to try to handle it with local resources first, then go to the State, which is where the National Guard would come in, and then go to the Federal Government and just work our way up. We were able to handle it exclusively with local resources, but I can see some scenarios where that might have become a viable option, Senator.

Chairman GLENN. In your situation, were oil supplies or gas supplies interrupted at all by this 4-day outage?

Mr. HARDY. No, they were not because we are almost exclusively hydrobased. So oil and gas just do not play a major role, really hardly any role, in our electrical power supply.

Chairman GLENN. Thank you very much.

Mr. HARDY. Thank you, Senator.

Chairman GLENN. We appreciate your testimony.

Our next witness is Mr. Charles White, Division Staff Executive, Power Equipment Division of the National Electrical Manufacturers Association.

Mr. White, we appreciate your being here. Proceed with your testimony.

TESTIMONY OF CHARLES H. WHITE, DIVISION STAFF EXECUTIVE, POWER EQUIPMENT DIVISION, NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION [1]

Mr. WHITE. Mr. Chairman, I am Charles H. White of the National Electrical Manufacturers Association. I want to thank you for this opportunity to present the concerns of NEMA and its members on the capability of the U.S. heavy electrical equipment manufacturing industry and the related capability of that industry to assist electric utilities in recovering from severe and widespread damage to the U.S. electrical system. Primarily, we are talking about those systems 242kV and greater.

NEMA, as you know, is the principal national trade association of the electrical manufacturing industry. The association has over 600 member companies manufacturing electrical products in the United States that are used either as components of, or as end equipment, in all major phases which generate, transmit, control, and utilize electricity.

Comments on capability and policy will apply to all of the major capital components used in such systems, but, for the purposes of illustration today, I will offer comment on large power transformers.

These are extremely large pieces of equipment made to the specific requirements of the purchasing utility. Because of their size, large manufacturing facilities, overhead cranes, and specialized manufacturing installations are required for their construction. Also required is equally large test apparatus and facilities. Under optimum conditions, it takes about 1 year to manufacture one of these large transformers. What happens to large power transformers is representative of the entire heavy electrical equipment industry.

---

[1] See p. 266 for Mr. White's prepared statement.

We are not talking about distribution equipment; that is, the gray equipment most often seen on poles or enclosed in green, pad-mounted cabinets in residential neighborhoods.

Chairman GLENN. Would it be correct to say that none of those are held in storage or in stock or in supply for possible use? We do not have any in reserve; is that correct?

Mr. WHITE. The distribution apparatus?

Chairman GLENN. Of the big transformers.

Mr. WHITE. There are none in inventory, no.

Chairman GLENN. It would take a year to build one?

Mr. WHITE. Yes, sir. It does not include equipment seen in the small utility parks known as distribution substations.

Since the early 1980's, annual energy forecasts have reduced the expected total demand for energy annually through the year 2000. Total demand for energy has declined as a result of conservation, improved product design, and energy efficient processes. However, the growth in electric energy demand has remained relatively constant at its long-term historical growth rate of 2 to 3 percent per year. Thus, we are less dependent on certain energy sources, but we are more dependent on electric energy to maintain our economic and material standard of living.

Mr. Chairman, the current and projected capabilities of the heavy electrical equipment manufacturing industry have been significantly changed by restructuring within the industry. In the large power transformer sector alone, nearly 40 percent of the U.S. production capacity has been removed in the last 30 months. This is due to utilities reaching the end of capital investment cycles which, combined with a slowing in the 7 percent yearly increase in electric energy demand of the last 1960's and early 1970's, has resulted in a decrease in demand for equipment used in electrical systems.

The reduction in the manufacturing capacity for heavy electrical equipment is a rational response to a down-sized domestic market for such equipment. However, it should also be noted that the reduction in domestic electrical equipment manufacturing capacity is also impacted by a worldwide surplus of such capacity, the causes of which are only partly analogous to the U.S. situation.

The problem is that today's domestic manufacturing industry is expected to support a utility capital plant base constructed, installed, and maintained on a manufacturing capacity which was 100 percent larger just 3 years ago.

Given the current utility capital plant base, any act which damaged as little as 10 percent of that plant would result in demand for billions of dollars of goods.

The bottom line, Mr. Chairman: Without a meaningful commitment by both utilities and Government to maintain a domestic manufacturing capability to support some identified surge in demand for capital equipment, U.S. manufacturing capability will continue to decline, becoming less able to respond to a crisis as time goes on.

One might be tempted to seek a solution by purchasing and storing needed equipment. However, such an approach overlooks the customized nature of heavy electrical equipment. Specifically, the design criteria and the application requirements for each such piece of capital equipment are so unique that it would be necessary to maintain a substantial number of individual replacement items. NEMA feels that the most effective way to inventory products is to have the manufacturing assets needed in an emergency. This approach has the added benefit of maintaining industrial viability and ensuring continued access to improved technology in product design, manufacture, and application.

What should be noted is that in spite of continuing erosion in the electrical manufacturing industry, the United States today is the world leader in heavy electrical equipment manufacturing, both in technology and economic efficiency.

The situation may be different in the near future because of economic circumstances and political decisions and, to a greater degree, because of unrestrained, unfair foreign competition in the United States as well as in the world electric equipment markets.

Foreign manufacturers of heavy electrical equipment have consistently, over time, been able to sell their products in the United States while their home markets have been effectively closed to U.S. manufacturers. In many cases, this institutionalized protection has provided substantial subsidy, enabling foreign companies to undercut U.S. goods in both the American market, as well as third-country markets. Such competition displaces U.S. producers and forecloses future commercial opportunities. Since 1971, the number of jobs in the heavy electrical equipment industry, just for the manufacture of large power transformers, has fallen from 10,000 to less than 4,000. The dilemma today is that once the investment in facilities, resources and personnel are redirected, our ability to refocus assets and resources under disaster conditions remains to be demonstrated.

Without viable markets or the expectation of such markets, U.S. electrical equipment manufacturers cannot make the investments necessary for a domestic electrical equipment manufacturing capability. In some instances, reduced production capacity will be partially offset by foreign manufacturers purchasing those domestic U.S. assets and then changing the production activity from manufacture to assembly.

The question for us is a very simple one. Does the United States desire to retain a domestic heavy electrical equipment manufacturing industry? Our trading partners have had occasion to address this question relative to their own industries. We know their answer: Concerted efforts by the U.S. Government to reduce the propensity of our trading partners from favoring their own domestic manufacturers have met with little success. This is due largely to their interest in retaining a domestic manufacturing capacity for security reasons.

The manufacturers stand ready to assist you in any way, as you continue your investigation on this issue.

Mr. Chairman, I would be pleased to answer any questions you have.

Chairman GLENN. Thank you, Mr. White.

Going back to the very high voltage transformers, the 750kV transformers, it has been our understanding that there was only one plant left which was capable of producing those transformers in this country. We were told that a couple of other plants could be brought on line to manufacture them. What is the status of our capability with the really big transformers?

Mr. WHITE. Mr. Chairman, that is correct. There is one facility that is currently on stream and can produce those assets on order. Other assets, two or three of them, have the design teams in place. They do not necessarily have the necessary designs or equipment available to initiate production as soon as time became available on a shop floor.

Chairman GLENN. How many transformers of that capacity would be used in the United States? Do you have any idea?

Mr. WHITE. Current production is about 100 of that class of transformer a year.

Chairman GLENN. That would be production. How many would be used, grand total?

Mr. WHITE. I think presently in service in the United States is a little over 4,000 transformers.

Chairman GLENN. Of that size?

Mr. WHITE. Yes, sir.

Chairman GLENN. Running up to that kind of capacity lets you reach out much further on your grid in your supply of electricity. How far out do you reach with power on a 750,000 volt transformer? How far can you reach, then, with that? Is there any rule of thumb?

Mr. WHITE. 750,000 volts, I assume you are speaking about DC, you could probably make a thousand miles.

Chairman GLENN. A thousand miles out. Okay.

You talk about unfair foreign competition in these areas. Are they subsidized in their production?

Mr. WHITE. Yes, sir.

Chairman GLENN. As opposed to us?

Mr. WHITE. Yes, sir.

Chairman GLENN. Who is the major supplier from abroad?

Mr. WHITE. Well, the major suppliers from abroad would be companies like Assaya, Siemens, Trafo Union—I think that is owned by Assaya now—those kind of major domestic manufacturers in their home countries. They have capacity far in excess of their domestic demand, and the policy was, as far as we can determine, to develop an industrial base permitting them to supply a world market.

Chairman GLENN. If you have one of those large transformers—which would be particularly vulnerable to attack, I presume; and we did have a terrorist attack of one kind or another, how would you cope when one of those transformers goes out? Are you capable, in general, of wheeling around that or getting power to circumvent that and coming back into the grid from a different source?

Mr. **WHITE**. Mr. Chairman, that really deals with the way a utility would handle restoration of service. The manufacturers can only respond to the decline in capital base that the utilities have.

Chairman **GLENN**. What would be your feeling on this, though? Is it your testimony that terrorist activity directed at these EHV transformers could make it impossible for domestic manufacturing capacity to meet the demand for replacement?

Mr. **WHITE**. Yes.

Chairman **GLENN**. What is the approximate size and weight of these transformers?

Mr. **WHITE**. I would prefer to submit an answer to that question in writing because it varies depending upon design parameters.

Chairman **GLENN**. All right. Well, my follow-up question was going to be on how you transport them, because, as I understand it, we do not even have enough rail cars to properly transport them if we had any real terrorist activity in this country. We only have 13 or 14 rail cars capable of taking the weight and size of the transformers, so I have been told. Is that your opinion?

Mr. **WHITE**. That is correct. I think 15 was the top number that was produced of the particular specialized equipment.

Chairman **GLENN**. All right. Thank you very much. We appreciate your testimony.

Mr. **WHITE**. Thank you.

Chairman **GLENN**. Our next witnesses are Mr. Michehl R. Gent, president, North American Electric Reliability Council; and Mr. David B. Hinman, Corporate Security, Alabama Power Company.

If you will proceed, Mr. Hinman.

TESTIMONY OF DAVID B. HINMAN, MANAGER, CORPORATE SECURITY, ALABAMA POWER CO.

Mr. **HINMAN**. Mr. Chairman, I am really honored to be invited to offer testimony before the Committee, and I will endeavor to present my views on industrial security within the public utility industry, and, in broader terms, what I believe is the typical environment for security professionals in the private sector. My experience in industrial security spans 27 years and two similar careers. One career of 11 years was in a former Bell System subsidiary, telecommunications, and my current career spans a little over 16 years in an investor-owned electric utility. I am currently responsible for the security of Alabama Power Company's personnel, buildings, equipment and electrical system. My testimony today will address security issues from an industry perspective generally rather than focus on efforts undertaken in any one company.

I believe it is important for me to describe for you the mission of a private sector security manager in contrast to our many associates in law enforcement. One significant fact is that we in security operate as private citizens when we represent our employer. We do not operate under "color of law," nor are we empowered to make arrests any more than any other private citizen. We obviously must be mindful of our liability exposure for our employers. We are not primarily in a reactive mode, responding to a complaint. We are primarily proactive, spending the majority of our efforts in preventive activities. If a building is to be built, we evaluate the site for exposure to crime. We meet with architects and engineers to consider security needs in the design of facilities. Our efforts include educational programs for our employees about drugs and alcohol, security of their homes and personal property, which generally enhances their security consciousness.

We conduct investigations when criminal activity is directed against our company, our property, or our employees. These investigations require a very close working relationship with law enforcement agencies, and we are, in effect, serving as a supplement to those efforts by local law enforcement. You may be surprised to learn that those of us in the private sector security outnumber sworn law enforcement personnel all over the country by a 2-to-1 margin. That is at either the Federal, the State and local levels of law enforcement.

Our responsibilities require that we stay abreast of new technologies in security hardware, computers, locking devices and access controls. Clearly, we must also be flexible to meet changing conditions so that our resources are channeled in the right direction. Our cost of operations impact the profitability of our company, and rarely do we contribute to profits. Our deterrent actions and preventive planning, although very difficult, may be impossible, to measure, reduce exposures to loss.

Most of us maintain and improve our skills and security knowledge through professional associations and industrial affiliations. The American Society for Industrial Security, as an example, has a membership of over 25,000 individuals internationally. The society conducts many seminars and workshops every year to keep members professionally trained. There is a continuing liaison with law enforcement and criminal justice leaders, and many of those enjoy membership in the Society. Many of us in the private sector present lectures at law enforcement academies, and law enforcement specialists frequently share their expertise in our internal training programs. Many professionals in private security also have previous careers in law enforcement.

Communications is an important part of any security plan or design and can expand or improve the efficiency and effectiveness of any security effort. Professional security managers have realized the importance of being capable of rapidly distributing information related to security concerns. In order to respond to this need, the American Society for Industrial Security has established an electronic bulletin board service which has the features of electronic mail and allows members and participants on that service to post alerts and bulletins for other members. The network is now operational and growing. I suspect that reports of these hearings will probably appear on our bulletin board as soon as they are available because this is of interest to the entire security community.

In responding to your questions, Mr. Chairman, about the physical security considerations for an electric utility, I must first offer my non-technical description of the facilities we use to serve over 1 million customers in my area of the country. We have a variety of generation sources, including a nuclear power plant, several coal-fired power plants, and more than a dozen hydroelectric dams. They are connected together in a massive grid of transmission lines so that each plant can supply energy to the total system. There are more than 9,000 miles of transmission lines and over 250 substations and switching points just in our area to assure reliability to our customers. The design, as I understand it, permits interruptions at any point on the grid without causing a loss of power to the end user, just as one broken strand in a spider web does not make it collapse.

Security plans and efforts related to the electric system itself focus and build upon this built-in flexibility. We know from experience with devastating natural disasters, such as hurricanes, ice storms and tornadoes, that the electric system can withstand severe damage and yet not collapse generally. The network of interconnections and switches allows operators to respond quickly to the loss of system facilities so as to minimize the area affected by any service outage that might occur. In 1979, for example, Hurricane Frederick severely damaged transmission lines and virtually destroyed the entire distribution system in our Mobile, Alabama, area. The storm isolated a major generating station and left us with 6,000 broken poles in our Mobile Division. Even so, the electrical system outside the damaged area continued to operate. There may have been a little minor, momentary interruptions, but all that was quickly put back in operation. Service to all of our customers in Mobile, virtually all, was restored within 3 weeks. I was there, and I thought it was an amazing piece of work.

Many factors can influence security planning for any specific electric utility. The geographic territory served, distances between generating facilities, climate, environmental and budgetary concerns are different for each utility. Some areas of our country are more prone than others to flooding, hurricanes, earthquakes, tornadoes and other natural disasters. The experiences of the past in dealing with these contingencies allow the security manager to add their own unique security requirements to any existing plans. The variables that exist preclude the development of any generic contingency plan that would fit everyone. We cannot fence and guard every transmission line and substation. The flexibility of the system is its greatest security. Our security plans must be built upon this fact in order to have maximum effectiveness.

Mr. Chairman, I thank you for the opportunity to appear, and I will be happy to respond to any questions you may have.

Chairman Glenn. Thank you, Mr. Hinman. We will have Mr. Gent's testimony first, and then we will get to questions.

TESTIMONY OF MICHEHL R. GENT, PRESIDENT, NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Mr. Gent. Thank you, Senator Glenn. I appreciate this offer to present testimony on the adequacy of Government programs designed to prevent or to respond to major interruptions of energy supplies that could be caused by terrorist acts, sabotage or natural disasters. What I will do today is try to summarize my prepared statement rather than read that.

Chairman Glenn. Your entire statement will be included in the record.[1]

---

[1] See p. 282.

Mr. Gent. You can see from that prepared testimony that I have grave reservations about testifying about such a sensitive subject as sabotage and terrorism in an open meeting. In fact, in my formal response, I offered to testify in a closed session and actually declined to testify in an open session. However, your staff has skillfully persuaded me of the errors of my way.

The record is clear that the electric utility industry has done extremely well handling disruptions caused by natural disasters, such as ice storms, hurricanes—as David just mentioned—and earthquakes. I can assure you that Government programs are in place and have proved to be adequate many times over.

From the headlines in newspapers, such as this Monday morning, all over the United States, and National Public Radio response, and from your staff, I assume that your primary interest today is the interruption of electricity supplies caused by sabotage and terrorism. Here, too, Government programs are in place, and electric utilities have addressed these issues.

It may be of interest to you to know how we have gone about accomplishing the assignment and this task of addressing this issue. The key lies in the way we are organized to ensure reliability of electricity supply. Every electric utility in North America is in one of nine Regional Reliability Councils. The nine Councils are organized to meet the needs of utilities in that region. Each is different. They vary from formal power pools to loose confederacies. These nine Regional Reliability Councils are owners of a not-for-profit corporation called the North American Electric Reliability Council. It is often referred to as NERC. NERC was formed after the Northeast blackout on November 9, 1965.

I feel I must emphasize that NERC is not an electric utility. It is not an association. It is not an institute, and it is not a Government agency. It is simply a company owned and operated by these nine Regional Reliability Councils. The members of the Regional Councils include utilities that are investor-owned, federally owned, rural electric cooperatives, State-owned and municipally owned. They account for virtually all of the electricity supplied in the continental United States, Alaska, Canada, and the northern portion of Baja California, Mexico.

The activities of NERC are directed by its Board of Trustees, who are generally the chairman and vice chairmen of the nine Regional Councils and generally CEO's or presidents in their own utilities. These nine regions form four major electrical interconnections or networks and sometimes referred to as grids. They are the Eastern Interconnection, the Western Interconnection, the Texas Interconnection, and Quebec.

Within each interconnection, there are several individual utility systems connected by alternating current transmission lines. This means that a disturbance occurring at any location in the interconnection will be felt by all the utilities that are connected to that interconnection. In the same way electricity transfers from one point in an interconnection to another point in that same interconnection, it will flow to some extent over each and every line, not just over the direct—contract—path of the transfer.

Our Operating Committee is responsible for creating what we call the "rules of the road." These are rules that allow all these electrical utilities to operate harmoniously together. The operating committee is also responsible for monitoring the networks for conformance to these rules and for investigating disturbances.

Through NERC, its committees, and the Regional Councils, the electric utilities of the United States and Canada have built and now operate the most sophisticated energy delivery system ever. It is also the most reliable energy system, and it is the most taken-for-granted energy system. And we want to keep it that way.

NERC has had only one mission in its 20 years, and that is to promote the reliability of the bulk electric systems in North America. We made the conscious decision that our purview also included sabotage and terrorism.

Three years ago, the National Security Council asked NERC to work with the Department of Energy to assess the degree of vulnerability of our electric systems and to devise a cost-effective program to mitigate that vulnerability. We did, but we approached it by looking at the degree of reliability and flexibility of our systems, as opposed to this buzz word "vulnerability."

After 2½ years of work by many individuals throughout industry, we have designed and are implementing a National Electric Security Program acceptable to Government and industry alike. The program, based on a quiet approach, with input from the electric utilities across the United States, serves as a model for effective cooperation between Government and industry. Our program makes use of old concepts and new concepts. It involves a close, ongoing working relationship with the FBI. It looks at all the elements of bulk electric supply systems, including the communications system, and it emphasizes operator awareness.

It all goes together as many pieces into a single program that does work and will work because it has enjoyed the grassroots input of electric utilities. It uses the resources that we already have and are available, and it is conceived as—I say again—a quiet program.

"Quiet" means that we have struck a deal with the Department of Energy and the National Security Council. They do not talk about this program in public, and we do not talk about this program in public. My testimony today is the first, and I hope the last, public utterance of our program.

We are obviously proud of what we have done. If you would care to have a closed session some time on this subject, maybe at a later time, I would be pleased to discuss the specifics of this program and its specific interaction between industry and Government. I think you would be impressed.

I know you are interested in the industry/Government interface. Mr. Badolato will follow me. He is from the Department of Energy, and he will explain the mechanics and the authorities, I am sure. But I would like this Committee to know that he should receive accolades for fostering this relationship and promoting the program that resulted.

Our relationship has been most unusual. Government identified a problem and asked us to solve it. There were no preconceived solutions, no agency liaison requirements, no agency oversight requirements, just a statement of the mission. I understand that our relationship and the results are being held out as a model for other industries to consider.

As follow-up work, Mr. Badolato and I have jointly briefed the Secretary of Energy, the acting National Security Adviser to the President, the Science Adviser to the President, and the Director of FEMA. I also previously mentioned that we have a relationship, an ongoing relationship, with the FBI.

If I could make a recommendation, it would be useful to institutionalize this approach that results in a trusting working relationship between industry and Government. More specifically, it makes sense to me to take some action that would ensure that this delicate trust is not undone by some future administration. I appreciate that this was mentioned in your opening remarks.

In summary, we have a program that addresses the issue, appears to be cost effective, has grassroots input from the electric utilities themselves, and is coordinated with the proper agencies of Government—a winning combination.

Chairman GLENN. Thank you, Mr. Gent.

We are in a situation where we can give good advice from the Government, and unless industry takes it, we will not really have any effective action being taken to reduce our vulnerability. Now, I appreciate the view from a utility standpoint that they are in a competitive business. How do we deal with this? The studies go on and say: "Okay, here is an area where we should be aware that a certain concentration of switching power, or whatever it is, is very vulnerable from a national security standpoint or against terrorism. But the utility may say I do not want to spend the extra $2 million to change that design." How do we take care of that?

Mr. GENT. I think we first have to start with——

Chairman GLENN. As I understand it, we do not have Government funds being given to subsidize a certain change that we think is dangerous, Is that correct?

Mr. GENT. There is a problem with any kind of funding other than those funds that are approved by the State commissioners for serving the customers.

I think first we have to establish that there is a vulnerability. I am not aware of the studies that you refer to.

Chairman GLENN. Well this indicates some difference between your testimony and Mr. Mullen's that I would point out. Your testimony says, "The electric utility industry's programs that deal with the possibility of sabotage and terrorism had its start following a reign of terrorism that began escalating in 1983. As a result, President Reagan appointed a task force headed by Vice President Bush to review the United States' program to combat terrorism. The task force's review of the current program to combat terrorism found the interagency system and the lead agency concept for dealing with incidents to be soundly conceived. However, the task force also determined that this system could be substantially enhanced through improved coordination."

Apparently, there was a feeling in Government, the NSC and your industry that there was a reign of terrorism about which you were concerned. That has been a concern of ours also. Mr. Mullen takes a little different view. He says in his testimony that:

What parallels may be found between the records of energy asset sabotage in preindustrial nations and in the U.S. reinforce my perspective concerning trends in the United States. Which is to say that there appear to be no indications that such trends will diverge in any significant way from what the historical record suggests.

I do not know whether that directly contradicts the other statement, but it also would lead me to believe that perhaps Mr. Gent is more concerned about the threat than Mr. Mullen's testimony would indicate.

Mr. GENT. Our concern, Senator, was with the Government's attention to these threats that had been accelerating around the world. He skillfully did not reveal in his testimony where the trend was going. However, Mr. Badolato has the numbers, and I was looking at them as he was testifying. Just eye-balling it, it would show that there might be an upward trend in the United States but very small.

Our concern is not with the events that we are experiencing now but with the potential capability that has been demonstrated to us by the Department of Energy in classified meetings.

Chairman GLENN. We are searching for the proper balance here, and I do not know what key role the Government has to play to ensure the provision of essential services. It is not only a national security matter, it is a general public welfare matter. We have DOE and industry working together in a relationship where DOE, as I said before, points out the problem, or the issue of potential multisite terrorism; then we leave it to industry to develop the low-cost solutions.

You apparently feel this is working well. I am not quite sure how it is to be spelled out down the line when you actually have to design a system and the number of transformers that go in, the number of lines and the development of alternate routing. Do we then go back in and assess what the industry is doing to take care of these concerns?

Mr. GENT. Senator, I think that most of the concerns for multisite sabotage are not considered in the design of power systems. However, events that are considered are probably as severe or more severe from a bulk power supply standpoint than multi-site sabotage and terrorism.

There are some things the industry can do, and we have a program to do those things. Some of those recommendations that were made to our board are in place now, and others are being implemented. This is the program I spoke of in my oral testimony that I would like to be able to tell you about, but I do not feel it is proper to do so in this forum.

Chairman GLENN. Well, we might want to follow up on that later.

Let me just say this for the record: I have not been as concerned about the electric power grid in the country and the electric supply as I have about some of the other energy supplies that I think have points along their routes that are far more vulnerable to major disruptions of a longer term and a much more cataclysmic nature, if you want to put it in those terms. In other words, we have some concentrations, and I do not want to state too much in an open session either, but I think we have some concentrations along those energy transmission lines that could really do serious disruption to our country.

I am sorry that the oil pipeline and gas pipeline people chose not to testify today, but I understand and share their concerns. However, we wanted them to testify in general terms as to what they felt the problem or the danger is, and we will be following up and getting more information from them.

The electrical grid in this country, or multigrids, have certainly proven very flexible in the emergencies we have had—natural disasters, storms, earthquakes, whatever. But, nevertheless, it just seems to me that it is very important that we do whatever we can; we plan ahead as much as we can.

One question in the report appended to DOE's testimony, entitled "Report of the Interagency Group on Energy Vulnerability," summarizing the past 2 years of NSEP planning, states:

> There is a Track A plan which focuses on ensuring that essential Government end-users of energy are identified, and that all Federal, State and industry crisis management plans are coordinated.

Are you familiar with that plan, and when will that be completed?

Mr. GENT. I think I am familiar with a portion of it as it relates to electric facilities. It has been under way for at least 2 years. It involves putting the local electric utility in touch with the critical facility that it serves, and then working out mutually agreeable plans.

Chairman GLENN. Well, there is also a Track B plan that is called for, which focuses upon longer-term action to reduce excessive vulnerabilities in the energy supply infrastructure. It calls for pilot studies and eventual national programs. Where are we with regard to that plan, do you know?

Mr. GENT. I could characterize the program that I have hinted about today as being a national program. I am not sure that that falls under that Track B. But I certainly would qualify it as a national program.

Chairman GLENN. Well, we will ask about those things later on. My time is up right now.

Senator Lieberman.

Senator LIEBERMAN. Thank you, Mr. Chairman.

Mr. Gent, good morning. I appreciate the balance that we are all trying to strike here between the responsibility of Congress to protect the national security and our concern about divulging too much detailed information that in itself compromises national security. And I think all of us are trying to respect those two goals while, at the same time, trying to fulfill our responsibility here. I hear your confidence that NERC certainly and the industry have taken steps that will improve our security. Let me just see if I can get a little more detail.

What assumptions about the likelihood of terrorist attack were used in determining our ability to respond to such an emergency? Did you posit probabilities, scope? In other words, what is the basis of your confidence at this point, based on your evaluation of the threat?

Mr. **Gent**. For our plan, we had to assume that it would occur. We did not come up with any probabilities.

I might add that skepticism was rampant among all participants.

Senator **Lieberman**. Skepticism that it would ever happen?

Mr. **Gent**. Yes. It was necessary to assume that it would happen and devise the plan and recommendations accordingly. But we never attempted to put a probability on the occurrence.

Senator **Lieberman**. Did you assume in your planning a multi-site-terrorist attack?

Mr. **Gent**. Yes.

Senator **Lieberman**. I do not mean to dwell on this, but I am curious about the skepticism. Not that any of us on this side of the table approach this with a sense of certainty, but we approach it with a sense of concern based on the real evidence of terrorist activities elsewhere in the world, some directed at energy and telecommunications facilities.

Mr. **Gent**. The first witness, Dr. Mullen, responded to a question that he had not—if I interpreted him correctly, he did not know of any organized multi-site sabotage attempt in a more modern country.

Senator **Lieberman**. Our concern, of course, has been that if you look at the evidence of behavior by terrorist organizations, including most recently the Pan Am Flight 103, you will see that those people are not playing by the rules that most of the rest of us are playing by. So I have approached these hearings with an attitude that we ought not to assume the worst, but we should be prepared for what has been happening.

Let me go on. To the extent that you believe our bulk electric systems are secure from terrorist attack, I want to understand in general terms what is the principal basis of your confidence in that security. Is it physical security of critical nodes in the system? Is it redundancy in the system? Is it the availability of spare parts?

I see you are laughing. I know you——

Mr. **Gent**. No, I am just wondering how I can answer that without——

Senator **Lieberman**. Well, try it. If you can answer it generally, I understand that. If not, maybe at some point we have to meet privately.

Mr. **Gent**. Certainly, the resiliency and the redundancy and the flexibility, and all those words, of the electric system is well demonstrated. I think the severity of possible damage from a hurricane far exceeds what any group of terrorist could ever accomplish, and we have demonstrated that we can handle hurricanes. So the redundancy and the flexibility is there.

Senator **Lieberman**. And that goes to the question of the ability to recover, correct?

Mr. **Gent**. Yes.

Senator **Lieberman**. Not so much to a prevention strategy, but to the ability to get the systems back on line.

Mr. **Gent**. Yes. If they, in fact, do go off line.

Senator **Lieberman**. If they go off line. Understood.

Can you comment at all on your evaluation of the physical security of critical nodes within the system?

Mr. **Gent**. Maybe Mr. Hinman would care to tackle that one. He is a physical security expert.

Senator **Lieberman**. Okay. Mr. Hinman?

Mr. **Hinman**. When we think of physical security, we typically think of taking something that is sensitive and building a building around it or a fence around the building and all these different perimeters under control. From what I understand, some of the components in a power grid system you cannot enclose them, and I am not talking about the fences going down the right of ways. I am talking about the transformers or switching points where there are electrical characteristics that do not lend themselves to be enclosed. We need air circulation and this sort of thing.

So, to that extent, I would say from a physical security standpoint, those—and nodes, I will comment on nodes. What we might consider a node in the electrical distribution system is quite different than what I would understand in telecommunications. If you have control points or control centers where all the switching capabilities can be directed, those have backup, those have sensitive apparatus, and they can be, and are typically, under adequate physical security measures. And if one of them fails, then there is a redundant system somewhere else that can back it up.

Senator **Lieberman**. The protection there is redundancy?

Mr. **Hinman**. Right. Now, as far as nodes, I think of telecommunications as if I need to talk to you, we need a link between the two of us, so that any facility that causes that link to be established can become a critical node. I looked at the electrical power system as being supplied with energy from a variety of generating sources. As Mr. Gent has said earlier, they must be synchronous and compatible, voltage-wise and that sort of thing. One little shift, it is like a ball coming in a pipe from one end and it goes out on the other end so the electrical system is an instantaneous thing, and it is not a path that allows you and I—we must have a path between the two of us or node in between us in order for us to get electricity that is out there.

Senator **Lieberman**. I believe that that is the red light, and not the sunlight, that is telling me my time is up.

Chairman **Glenn**. I have a couple more questions.

Mr. Hinman, what happens when there is an alert received from DOE or the FBI based on intelligence information? What happens to that? I know it would depend on the nature and information contained in the alert, but do you have a standard procedure you recommend to the industry for that?

Mr. **Hinman**. Well, we have had discussions about this. I can comment on it from the standpoint of what happens to me if I get such an alert. May I do that?

Chairman **Glenn**. Sure.

Mr. **Hinman**. We have had some of these, and the formal communications within the company have not been in place. We had some surprises. We would get an alert, and I do not know about it. The people who got the alert call me, so we do not know who else it was disseminated to. So there has been some confusion generated and created for me where alerts came to other elements of my company management, and I was not aware of it.

But, basically, as a security professional, I would expect to evaluate such an alert or get a professional evaluation, typically from the FBI, as to whether or not my particular facility is a target. After that assessment was made, I would then generate the necessary communications within my company to put into place our emergency management teams who are accustomed to getting together when we have other natural disasters or labor disputes.

Chairman GLENN. Do you have your own security force, or would you depend on the local police in a case like that?

Mr. HINMAN. Well, we have our own in-house security operation. I prefer that because it gives me the flexibility. If we have a critical problem in one area of our service area that deserves some increased manpower, I can draw that manpower from less critical areas, although that opportunity presents itself for contract agencies as well.

Chairman GLENN. But, if you had one of these big EHV transformers or similar equipment, and you thought there was danger to that thing, would you go out? Are your people authorized to carry weapons and actually protect something like that? Or, do you have to call on the local police?

Mr. HINMAN. In Alabama, we are authorized to carry firearms.

Chairman GLENN. Is that customary across the country, though, in other States?

Mr. HINMAN. No, sir. It is not.

Chairman GLENN. Well, then are they just dependent on local police? If they would get an alert, they would call up the local police and say, "we think there might be a problem here and please protect us," and that is it?

Mr. HINMAN. No, sir. I do not think I would involve law enforcement unless I had a specific target that had been provided to me. If somebody gave a general threat, there would be certain actions I would take that I really would not feel comfortable discussing here, but we would have a response and we have a planned response.

Chairman GLENN. Well, how useful are DOE's alerts? Have they been useful, and is it the type of information that you can really act on?

Mr. HINMAN. Well, if you say DOE alerts, I understand that the alerts, or at least the ones I have seen in the last couple of years, originated in the Department of State. DOE was the funnel through which the alert went to NERC. When it got to me, it was of questionable value.

Chairman GLENN. And what did you do on one like that? Did you actually take any physical action of putting people out on certain sites, or turn it over to the local police, or did you just take it as some information you had been given and that was it?

Mr. HINMAN. I did not take any action on any of the alerts because they were not specific enough; they contained information that I think was generally available in the media. It was not anything specific to my industry. There was confusion sometimes because of the method of dissemination within some of the organizations—not DOE, but within our own company, pieces of the message got cut off or incomplete communications. Where there was a reference to Southeast Asia, it came out as "Southeast."

Mr. GENT. Maybe it would proper for me to comment.

Chairman GLENN. Southeast could be United States, not Asia. Is that what you are saying?

Mr. HINMAN. Well, that is right. And I really would defer to Mr. Gent on this.

Chairman GLENN. Fine. Mr. Gent, and I am sure Mr. Badolato will want to ask him a little bit as to whether we need some improvement in that area.

Mr. GENT. The alerts themselves, the words might have been of questionable value. However, the exercise was not. It allowed us to establish a communications net and sort of wring it out. This is all now part of our program, and we also have put into place a way for the local utility, upon receiving the message, to determine how it affects it.

Chairman GLENN. Well, I can understand that you need to have a lot of flexibility on it. But is this an adequate system the way it is set up and working right now? It sounded to me as though it is hardly that——

Mr. GENT. It works fine.

Chairman GLENN. It does?

Mr. GENT. Yes.

Chairman GLENN. Well, what do you do then? Let us say you are running a utility, and you are the president of that utility. You get an alert from DOE. Then what do you do with it?

Mr. GENT. Well, there is a procedure to handle that that I cannot discuss in open session. But it would not be the president that got it.

Chairman GLENN. Are there different classifications of warnings, different classifications of alerts?

Mr. GENT. No. They are all declassified. They are unclassified right now. That is why we have to have a verification——

Chairman GLENN. They are all unclassified, but are there different levels of warning? In other words, is there an alert that means you are about to be attacked as opposed to one that indicates the terrorist threat has gone up worldwide? Those would be two different levels of concern.

Mr. GENT. I would defer to Mr. Badolato on that.

Chairman GLENN. OK. We will get into that one a little bit later, then, too.

Do you have more questions?

Senator LIEBERMAN. Yes. Thank you, Mr. Chairman.

Mr. Gent, earlier we talked about the ability of the system to defend itself or to recover, and I know we were making comparisons to some of the natural disasters like hurricanes. Correct me if I am wrong, but my sense is that the typical act of God, such as a hurricane, would not knock out a transformer. Is that correct?

Mr. GENT. It could. I do not know.

Senator LIEBERMAN. That was my sense of it.

Now, my question is based on some of the testimony of officials from Seattle and the others who testified here this morning, who suggested that a transformer might take as much as year to put back on line. Does that not worry you? What kind of confidence can we have in avoiding mass disruption and tremendous economic loss if that is the case?

Mr. GENT. There seems to be a perception if you take a transformer out everybody is out of power forever until you can replace it.

Senator LIEBERMAN. Yes, tell me about it.

Mr. GENT. That is not necessarily true. The system can always be re-rigged or jerry-rigged. You can serve it many, many different ways. I doubt seriously that losing a transformer would curtail service until you could replace the transformer. There are alternate ways of providing power into areas.

In the case of Seattle, that is probably the absolutely most difficult because it is underground. Those are the most difficult.

Regarding lead time to replace a transformer, it is my understanding that if you had the design—and almost everybody has the design—and if you were given the raw material and the availability of the raw material, you could make one in 6 to 8 weeks. The difficulty comes in that you cannot economically do so. It would have to be some kind of an emergency, all economy set aside. As I understand it, you have to set up a manufacturing line and justify producing so many units to be able to even begin production, and that is where the year comes in.

Senator LIEBERMAN. Should we be inventorying or stockpiling transformers? I understand that there is an extent to which they are custom made.

In other words, is there anything we can do to create some kind of backup for that part of the system, which would seem to have the most devastating impact on energy systems if it were knocked out?

Mr. GENT. There are already spare transformers all over the country. Part of our program is to look at those transformers and try to classify where they are.

Senator LIEBERMAN. So your program has dealt with this particular problem as well?

Mr. GENT. Of course.

Senator LIEBERMAN. Which is the availability of backup for transformers.

I asked a general security question before. How about the need, therefore, to try to provide some extra measure of security to the transformers? Have you dealt with that? A preventive action.

Mr. GENT. We certainly talked about that, but I think it is virtually impossible. We are talking about a unit that can be as big as this room.

Senator LIEBERMAN. Right.

Mr. GENT. Security comes long before they get to the transformer, and there are a number of programs that are being considered or implemented, like the neighborhood watch program that was mentioned by Dr. Mullen earlier. That is a possibility. We have crime scene awareness programs.

Senator LIEBERMAN. Right.

Mr. GENT. So our programs are more preventative. We are not doing anything to protect the transformer per se. That is virtually impossible. There might be some considerations about where the spares are located and that sort of thing.

Senator LIEBERMAN. And that is your catalogue that you are bringing together?

Mr. GENT. That is part of it, yes.

Senator LIEBERMAN. Mr. Hinman, what is the typical security around a transformer at a typical power station or generating facility in America? Is access to the site typically limited? Do you need identification to get in? Are there guards, typically?

Mr. HINMAN. I would think the most typical would be a semiremote area. Our neighbors do not want a big humming transformer sitting out there next to them. They are strategically placed for electrical reasons. They are generally, well, almost without exception, fenced. Those fences are designed to keep cattle, dogs and children out of there because it is potentially dangerous for people to walk around or climb into that area.

Basically, they need air circulation. Most are equipped with large fans that are used from time to time to aid the cooling process. And so that pretty well requires that they be in an area where there can be some air circulation, forced or otherwise.

Senator LIEBERMAN. Typically, there would not be security personnel on site on a 24-hour basis?

Mr. HINMAN. I cannot think of a circumstance that would justify that.

Senator LIEBERMAN. One other line of questioning for you, Mr. Hinman. Suppose that the worst case did occur and there were a terrorist attack on a facility that was within your jurisdiction. What is the Federal role? Do you think you can handle it yourself, or is there a clear line of access to Federal assistance to help you through?

Mr. HINMAN. Well, there is a clear line, and it has been well developed, as far as the liaison with Federal authorities, to respond in the event we have a situation. The thing that I place the greater value on is their ability to gain intelligence and alert me directly before the event takes place. And I rely a lot on that.

Senator LIEBERMAN. Who would you go to at the Federal level, let us say after or as an event is occurring? Which Federal agencies?

Mr. HINMAN. Well, I would start with the FBI. Typically, if it is a localized situation or one that is identifiable from the standpoint of where something may happen or just has happened, then we have got support from the local law enforcement and State law enforcement people. But I would have that contact within my own area, and it is already established.

Senator LIEBERMAN. If I may, Mr. Chairman, just one more question.

There was testimony from Mr. Hardy, suggesting that Seattle was lucky because the fire there did not rupture any of the city's transformers, which "would have produced considerable damage and risk, either through the immediate explosion that would occur or the release of potentially PCB-laden smoke."

Do you or do energy facilities typically have emergency plans to deal with those possible effects of an explosion at a transformer?

Mr. HINMAN. We have very comprehensive plans, and we have had an exercise on more than one occasion. There are currently the contingencies for dealing with hazardous materials. Those are factors we have to look at, and we work very closely with both the

State fire people, local fire people, on controlling those effects of any fire around our facilities.

Senator **LIEBERMAN**. Thank you.

Chairman **GLENN**. Thank you very much, gentlemen.

We will go on to our next witness: Mr. Edward V. Badolato, Deputy Assistant Secretary for Energy Emergencies, Department of Energy.

Mr. Badolato, welcome to our hearing. You have heard a lot of the concerns here this morning. I am sure you are anxious to address them. We welcome your testimony.

Let me just say in advance that I will have to leave shortly to appear before another Committee, where I am to give some information on behalf of the Governmental Affairs Committee. They are running just a little bit behind schedule, but I will have to leave in a few minutes and will turn the hearing over to Senator Lieberman. I will try and get back before the end. If not, he will have the chair until the end. I am sorry that we have that interruption, but that is the way it goes.

I look forward to your testimony.

TESTIMONY OF EDWARD V. BADOLATO, DEPUTY ASSISTANT SECRETARY FOR ENERGY EMERGENCIES, U.S. DEPARTMENT OF ENERGY [1]

Mr. **BADOLATO**. Thank you, Mr. Chairman.

Mr. Chairman and members of the Committee, I appreciate this opportunity to appear before you today to discuss the vulnerability of U.S. energy systems and what we in the Federal Government, in cooperation with the energy industry, are doing to make these systems less vulnerable to disruptions. We appreciate your understanding of the sensitivity of the details of the subject, and I will orient my remarks to accommodate these sensitivities.

The Department of Energy has made substantial progress in support of the administration's energy emergency policy, which is, essentially, to ensure that our Nation has an adequate supply of energy at a reasonable cost. DOE's non-nuclear energy emergency preparedness program is aimed at reducing the Nation's vulnerability to energy supply disruptions and enhancing our ability to respond should a disruption occur.

Today, the United States is better prepared than ever before to deter, as well as to respond to, any energy supply emergency arising from foreign oil disruptions or from domestic incidents involving our basic energy infrastructure.

Despite this initial progress, we are not complacent. We take this challenge very seriously. There is a wide spectrum of potential threats to energy supply systems, from a multitude of causes, ranging from natural disasters to terrorism, and even war, which requires constant vigilance and readiness. The subject of my testimony today will be how the men and women, of the Department of Energy's Office of Energy Emergencies, are ready 24 hours a day, 7 days a week, and 365 days a year to deal with these potential threats to our Nation's energy systems, and ensure that our country has adequate supplies of energy at a reasonable cost.

---

[1] See p. 296 for Mr. Badolato's prepared statement.

Over the past 2 years, DOE has taken decisive steps to substantially strengthen and reorganize the Nation's ability to respond to energy emergencies. We have reorganized our staff; developed new emergency organizations and procedures; revitalized our interaction with the energy industry; and developed a close working and planning relationship with each of our State energy organizations—all done with existing resources.

These accomplishments can be summarized in the following four major categories: First, the internal reorganization of the DOE's emergency preparedness structure; second, DOE leadership of the Federal role in energy emergencies; third, an overall framework for dealing with energy systems' vulnerabilities; and, fourth, strengthening cooperation with industry and the States in planning for energy emergencies.

I would like to say a few words about each of these and then respond to your questions.

First, the internal reorganization. The Department has developed procedures for and exercised its energy emergency management system [EEMS], a powerful new management tool incorporating departmental emergency response capabilities and crisis management systems into a structurally integrated framework, to facilitate its ability to respond to foreign or domestic energy emergencies.

Second, the DOE leadership of the Federal role in energy emergencies. The Department is the lead agency of the Federal Government's interagency program to deal with energy vulnerability, and we chair a vigorous governmental effort whose purpose is to assess energy vulnerabilities; evaluate the response options available; and then analyze the consequences of emergency scenarios.

Third, the overall framework for dealing with energy systems' vulnerabilities. We have developed an overall strategy for dealing with energy vulnerability, which includes a cooperative energy vulnerability assessment program to work with the energy industries—that is, electricity, oil, gas and coal—to study the domestic industry's facilities, security and restoration capacity; to develop an automated vulnerability assessment system technology, the AVAST program, which was developed by our laboratories and is being made available to help industry plan for its own security; and an outreach program which allows us in DOE and the energy industries to shape and share information on how to better reduce potential vulnerabilities.

Fourth, the strengthening of our cooperation within industry and the States. The Department has revitalized its National Defense Executive Reserves, those industry executives who augment DOE's energy crisis management during national security emergencies. We have done this by aggressively recruiting members. We have established new training programs, and we have arranged for them to participate in our Departmental tests and exercises.

Additionally, nearly all of the States and dozens of industry representatives have participated in regional emergency preparedness seminars to enhance communication and cooperation with State and industry emergency planners. Also, a steering group has been formed around the United States consisting of top State energy office directors to continue this collaborative approach to energy emergency planning.

In conclusion, we have created a means for unprecedented participation by Government and industry in assessing and mitigating energy system vulnerabilities. Also, a strengthening of the Federal/State preparedness activity has been achieved in the past few years. The Department of Energy, through its Office of Energy Emergencies, plans to continue its priority program to mitigate energy supply system vulnerabilities and ensure that our country is ready to respond to any energy emergency.

Mr. Chairman, I will be happy to respond to any questions you may have at this time.

Chairman GLENN. Thank you very much.

I would like to ask first about the physical security responsibility that was given to the FBI in Executive Order 12656. They were tasked with the duty to assist heads of Federal departments and agencies, State and local Governments, and the private sector in the development of plans to physically protect essential resources and facilities. Mr. Woloshin, Associate Director of National Preparedness for FEMA, also gave testimony to that effect, that responsibility was being given to the FBI.

Now, does this change DOE's primacy in any way? Are you working with the FBI, or did you give them that responsibility and then you no longer have anything to do in that area?

In other words, what is DOE's continuing responsibility and what has been given to the FBI?

Mr. BADOLATO. Mr. Chairman, the Secretary of Energy has statutory responsibilities to ensure the energy security of our country, both in the domestic sense and in regard to any foreign energy situation. In that regard, we have the authority to do this, and we intend to work closely with the FBI to ensure that, in the energy sense, we have the capability to provide them with the overall planning effort and the detailed understanding of what goes on in the energy areas.

With this in mind, we work very closely with the FBI. The FBI headquarters has a relatively small staff—I believe it is only two people—that are attempting to do this job. They may increase later, but we presently work very closely with them. We invite them to participate in our energy emergency exercises. We also have their special agents, in the field, participate in our exercises. We do not see at the working level, nor at the higher level, a change in that cooperative relationship.

Chairman GLENN. OK. I was concerned about the part of your abbreviated statement that did not cover it—let me just go back here a second.

On the second page of your full statement, you quoted from the 1986 report entitled "Public Report of the Vice President's Task Force on Combatting Terrorism." You quote from the report and say:

> Our vulnerability lies, ironically, in the strength of our open society and highly sophisticated infrastructure. Transportation, energy, communications, finance, industry, medicine, defense, diplomacy and Government itself rely on intricate interrelated networks. Given these inherent vulnerabilities, and the fact that Americans

> are increasingly the targets of terrorist attacks outside the United States, it is apparent that a potentially serious domestic threat exists.

You go on then to quote Mr. Oliver Revell, who is Executive Assistant Director of the FBI, out of his address to the National Association of Chiefs of Police in October of last year. He stated:

> The United States . . . is vulnerable to terrorist criminal activity. Potential terrorist support networks are in place in the United States and certain international terrorists have the motivation to commit terrorist acts . . . the possibility of international terrorist committing acts in the United States continues to exist.

That states the problem pretty well. I agree with that.

You heard the questions a little while ago about what happens to these alerts. What happens when you get information that something might occur? Are there categories of alerts? How do you put them out? What do you expect the industry to do? Are they dependent on local police? Do you give any assistance beyond that?

What happens to these things? What number, if you can give us that, of these alerts go out each year? Are there so many that they are virtually ignored? Or do you categorize them in ways that would really motivate action at the other end of the line?

Describe that system for us.

Mr. BADOLATO. I would be delighted to do that, Mr. Chairman, because there is some misunderstanding of this, which I hopefully will be able to clear up.

First, we must distinguish between what is an advisory and what is an alert. This country's system of protecting its critical assets has always had a domestic alert system, and that alert system has been and is continuing to be run by the FBI. The FBI will make specific alert notifications when it has information about targeting of infrastructure in particular portions of the country. It has and will continue to do that. That is promulgated by them, and I would assume that they would be able to provide that information.

We did not have a system to do advisories, and that is what we have developed. Every notification that we have made to the industries has been an advisory; that is, an advisory about general areas of concern. We found that the State Department had notified U.S.-owned foreign industry and businesses about potential terrorist problems and part of their notification had contained some information that this could also take place in the United States. We became concerned that this information was not being distributed because it was below the specific targeting information of an alert that we should promulgate advisories.

With literally thousands of energy organizations and industries around the country—NERC alone has over 3,400 utilities—we went directly to the industry representatives. We went to NERC, API, American Gas, and the National Coal Association and said: Can you help us with your hotlines to get this information out if we can provide you an unclassified system for describing that there are areas of general concern that we would like to let the industry know about?

They were very, very helpful. There were some rough spots in the beginning. This had not been done before, as you have heard Dave Hinman say, and some of the security directors were concerned because the alerts were delivered in an administrative fashion and their boss got it, or the administrative officer or the comptroller got it and the security guy was getting called by them and was being notified last. I agree with him. I think I would have been put out by that, too.

Additionally, in the retyping and transmission of these advisories, there were some garbles and things like that. We worked hard with the various industry organizations to get this under control. We filled a vacuum. We not only filled a vacuum, but my marching orders were, when I took over this job, to ensure that we would never have to go before this body or the American people and say that we had information, even general information, that something was being perpetrated by enemies of the United States on our energy infrastructure and, that we stood idly by and did not do anything about it.

With that in mind, I would like to say that our advisories were exact repeats of what the State Department sends out to our U.S. companies overseas. These advisories contain information indicating that this foreign threat can involve the domestic industries of the United States.

With that in mind, those threats, those problems, those advisories that we put out are thoroughly coordinated at the highest level of the intelligence community in Washington. The FBI takes part in that. However, agents out in the field may not be involved.

Consequently, I am prepared to submit to you for the record, if you would like, a detailed list of the advisories we have sent out to date. Essentially, the numbers are several in 1987 and several with updates. And as we issue the advisories, we had a goal, if the intelligence community and the State Department feels this is continuing, we try to provide an update every several weeks so the industry knows we have not forgotten about them.

Chairman GLENN. We would like to have that, and we will include it in the record.[1]

My time is up, and I am going to have to go to the other meeting. Senator Lieberman will chair.

Thank you very much.

Senator LIEBERMAN [presiding]. Thank you, Mr. Chairman, and thank you, Mr. Badolato. I appreciate your testimony. And if I may say so more generally, I appreciate the attitude that you bring to the position. Not wanting to be an alarmist or manufacture a concern where it does not exist, nonetheless there seems to be enough in our world to suggest that there are those who would try to do damage to the United States by striking not at military targets but at civilian infrastructure targets, telecommunications and energy targets particularly. So it gives me some encouragement to hear your testimony and hear that you are out there working for us, for the American people.

I take it that you find it plausible that there might be a serious threat to energy systems within the United States from terrorists.

Mr. BADOLATO. I take the potential threat seriously, for a number of reasons. As you heard Dr. Mullen say—and his numbers are about as good as there is in the intelligence world, as he collects this information—since 1980 there have been approximately 8,000 attacks against energy systems around the world.

---

[1] See p. 351.

We have been lucky in the United States. But the individuals that do this are only a plane ride away. I am accused by some people in the industry and other places and parts of the Government as being an alarmist and a man who is trying to call attention to this. But, generally speaking, when we get into the facts and we talk to the people in the industry and the other parts of Government, they understand the seriousness of what is going on.

I take the threat seriously because there are terrorist groups inside the United States and there is international terrorism. We just sentenced a man yesterday who was part of an international terrorist-for-hire group that was accidentally caught on the New Jersey Turnpike. We gave him 30 years for being a member of the Japanese Red Army and coming to the United States and possibly, we think, getting ready to perpetrate terrorist acts inside the United States as part of an international terrorism network.

I take it seriously, Senator.

Senator LIEBERMAN. OK. Thank you. When they call you an alarmist, please take it as a compliment. I would rather have you be called an alarmist than someone who is complacent.

Let me just explore for a moment the fundamental role that you see for DOE. As I understand it from what we have heard, DOE's activities have been based on creating a working relationship with the industry, pointing out the problem, the issue of potential damage, and then essentially encouraging or perhaps leaving it to the industry to go from there.

If you would step back for a moment and think about the future and the best of all worlds; is that the best role for Government? Is there a more active role for Government to take in protecting our energy systems from possible attack?

Mr. BADOLATO. In looking at this program that we have developed, it is a 4-phase program which essentially involves, in the first phase, exercises and case studies and assessments to really know what the energy vulnerability situation is insofar as its likely impact on national security. Then in the second phase, reaching out to industry and saying we have found this out, we are coming to you. We know intelligence. We know national security. You own and know how to operate those industries. We have some concerns. Will you look at this yourself?

Next is the third phase, in which industry reevaluates their vulnerabilities. NERC worked for about a year-and-a-half doing this.

We then take what they give us, coordinate our information and we analyze it to see if it is useful.

After the third phase, industry comes back and says we have looked at our vulnerabilities and we have looked at mitigating measures. We are implementing these fixes and things of that nature.

This, then brings us to the fourth phase, which may require us to sponsor additional vulnerability mitigating initiatives. I am not prepared to say which specific initiatives at this time; we have not gotten there yet. The electric industry is our model for this and they are just completing their third phase.

When we finish, there may be a more proactive role for that, but I am not prepared to say that yet.

Senator LIEBERMAN. Understood. What might it include?

Mr. BADOLATO. Well, there may be things we could do if the industry needs help. You have to remember that we have two highly regulated industries, and gas and electric are included in this. Oil is a different story. They may need assistance with the States and the Public Utility Commissions to, for example, allow some security activities and things to be brought in under the rate base.

I am not an advocate of that, but I am saying these are things which are hypothetically possible downstream.

Senator LIEBERMAN. Do you think there would be any need for the Government at any point to try to maintain an inventory of backup parts, replacement parts, or are you satisfied that the industry itself is doing that as well as it can?

Mr. BADOLATO. Mr. Chairman, you mean an actual physical inventory or only to better understand where they are?

Senator LIEBERMAN. I would say both. But my question had to do with the physical inventory, so let us start with that one.

Mr. BADOLATO. Well, the physical inventory itself, I have to tell you, from analyzing and getting involved with what is going on, the industry is not really sure how many spares exist right now throughout the United States.

First, before I can effectively answer that, we would have to understand exactly where we are. We have heard the offshore problem discussed, the lack of manufacturing base, and things of that nature. We have to have much more definitive information on this, and I think NERC is moving toward this. The electric area is probably one of the more critical areas, more so than some of the compressors and specialized pumps and valves and things in the other industries. But we have got to get our hands around it, and then I think we can answer the question as to what should be done about physical inventories.

Senator LIEBERMAN. Are you asking that question now? In other words, are you trying to gather that information now from NERC?

Mr. BADOLATO. It is my understanding that information is being put together by NERC. We have also done some analysis of it and some overall looks at the situation to get a feel for it.

Senator LIEBERMAN. How about the other kind of inventory? Does DOE have an inventory of critical facilities, a list of locations in the country where you have special concern for vulnerability?

Mr. BADOLATO. We are working on this, and you heard discussed—what may be a little bit confusing to some who are not aware—a Track A and a Track B. First, Track A essentially is up front, those critical assets in energy systems which—if disrupted—could impact on national security. We are working hard on that. We have had tremendous activity here. We have done a lot of exercises; we have done a lot of analysis on this. My staff is working very hard on this with FEMA and with the Department of Defense.

So, in that sense, we are working toward this. That is, to look at our critical energy facilities and make sure we are doing our part from Energy. All the critical energy facilities, that is, in electric, in gas, in oil and coal industries.

Next, we intend to move this along into Track B and to look at, from a national standpoint—not just national defense—our overall strength and well-being, both industrially and economically. For this, we must understand our infrastructure. We would hope to be able to work with FEMA very closely on this in doing this.

Senator LIEBERMAN. I take it from what you said a moment ago that there are some occasions when the industry has proposed actions which you found insufficient, and there has been some dialogue about those. Is that correct?

Mr. BADOLATO. Well, I think give-and-take is important. But, generally speaking, you have to understand that, Government and industry—please do not think I am trying to lecture you, Mr. Chairman.

Senator LIEBERMAN. No, go ahead.

Mr. BADOLATO. We have a give-and-take situation and industry has its position. We do not always see eye to eye. I appreciate Mike Gent's kind words, but we do not always see eye to eye, but now we are talking about these security topics. I think in the long run we will always be the Government and they will always be industry. But now, for the first time—and I have to tell you, I have letters and testimonials coming in from people in the industry saying it is the first time that we have had an opportunity for Government and industry to sit down to try to work out these emergency problems. We have also had an opportunity to sit down with people from State energy offices and regulators and people from emergency offices, and with industry for the first time in a non-confrontational way to get at this problem. This is going on now all over the country, and we are very proud of that.

Senator LIEBERMAN. I understand, but just as you say, Government and industry are coming out in slightly different ways. But, obviously, we have a common purpose here.

Do you ever feel that DOE should have some more specific statutory authority to compel certain actions from industry in the interest of national security?

Mr. BADOLATO. Mr. Chairman, right now we have a number of statutory authorities. In my estimation, in studying this very hard and exercising—and we have run literally dozens and dozens of emergency exercises so that there is not very much that can happen that we do not have a feel for, including the statutory authorities of DOE's Secretary and what he is personnally supposed to execute and those that he has delegated down to me. And I think that our authorities right now are fairly good. I think they are adequate, in fact.

Senator LIEBERMAN. You are satisfied at this point?

Mr. BADOLATO. I am satisfied at this point, sir.

Senator LIEBERMAN. Let me ask a few more internal questions. Yesterday, we focused on telecommunications concerns, and the National Communications System, NCS, we were told, has an annual budget of approximately $75 million. I see you are smiling. You probably know which way this question is going.

Your office addressing energy concerns has an annual budget of $6.2 million. Understanding the budgetary context in which we are operating, is that adequate? Forget the budget pressure. Just think in terms of national security. You have got less than a tenth of what NCS has. Is that enough for you to do what we want you to do?

Mr. **Badolato**. Well, Mr. Chairman, I would like to say a few words that Dwight Eisenhower used to tell the troops. He said, "It is not the size of the dog in the fight, but the size of the fight in the dog." With that in mind——

Senator **Lieberman**. If I may say so, respectfully, you seem like a pretty feisty dog to me. [Laughter.]

Mr. **Badolato**. Thank you, sir.

We have in the Department of Energy a $6 million plus budget, we have a small, well-trained staff. We maintain the emergency processes, and we are prepared to expand rapidly. We chair committees. We bring in people. We are the conduit. We are the keepers of the lamp on emergencies, if you will.

Now, I assure you, as I have assured the Appropriation Committees that we talk to, that we are squeezing every nickel of value out of that budget for emergency preparedness. We think that we have adequate funds to do what we are doing now at the pace that we are doing it.

Senator **Lieberman**. OK. I understand the answer, and I appreciate it.

How adequate, then, is the coordination between energy industry/DOE on the one hand and telecommunications/NCS on the other? For instance, some of the scenarios we have discussed here and the staff has pursued, focus on the problem of restoring emergency circuits needed for the electrical or pipeline industries if there were an assault—intentionally, or even accidentally—on both grids. Is there adequate coordination on this point?

Mr. **Badolato**. I would say yes. Granted, NSTAC and we understand that you cannot have communications without electricity; on the other hand, you cannot have electricity without communications. It is too important.

Senator **Lieberman**. Right.

Mr. **Badolato**. We have Ben Morris, who appeared before this Committee yesterday, as a member of our energy vulnerability group that DOE chairs. We are heavily involved with him and our staff is working closely with his staff. We consider ourselves to be a broker between NSTAC and NERC, also, who have begun to work together, and we have fostered that over the last year plus some time.

We think that right now, from our perspective in the Government, that the communications industry and the electric power industry are working together in a very useful manner. They have a lot of work that they are planning to do and cooperative efforts and so forth, and we are very encouraged by that.

Senator **Lieberman**. I appreciate hearing that because one of the elements of testimony yesterday which troubled some of us on the Committee was the apparent increasing consolidation of telecommunications facilities; that is to say, the concentration, because of technological developments, on limited series of paths, eliminating what I have now come to call redundancy. I guess that is the term of art. Basically, I would say different ways to do the same thing. And also the affect that economic competition within telecommunications has had on security concerns.

The other point is the interdependency of both the energy and telecommunications sectors, and that seems to be growing, too. So I appreciate hearing that you feel that there is adequate communication between the two elements of our Government involved. I think it is critical.

If I may ask you to just step back just a little bit. One of the things that struck me as I prepared for these hearings, in reading a Committee staff report, was the wide range of Federal agencies involved and the enormous number of alphabetic acronyms that exist. Part of what I have tried to do in these hearings is to put it all together and see not only if it is working okay, but whether it could work better.

I understand the difficulty because you have a particular position now, but is there something more that the Federal Government could do to coordinate the national preparedness to respond to terrorist attacks. Is the structure adequate now?

Mr. BADOLATO. Right now I think we have a very good structure. I will speak specifically using energy facilities as a model, which I am qualified to speak to.

At the present time, we have a good structure at the national level with the capability at sub-Cabinet, working through the NSC, National Security Council, to deal fairly rapidly with problems which may arise. That is, we can call together in just a few hours, consider some important activities, and we have done this and exercised it, and we feel comfortable about that.

Senator LIEBERMAN. Can I intervene just a moment?

Mr. BADOLATO. Yes, sir.

Senator LIEBERMAN. One of the important things really in any organization, but certainly when you are dealing with critical questions such as you deal with, is to locate responsibility. Is it fair to say that the central responsibility for the kinds of concerns that have been the focus of these hearings rests with the National Security Council now? I have seen all the charts. Is that where the responsibility for initiation and ongoing oversight of our protective systems rest?

Mr. BADOLATO. During the last Administration, the NSC has certainly taken the lead in this area on national security emergency preparedness for mobilization, for civil defense, and for energy vulnerability, and have done a very credible job. In our particular area, we had a very vigorous, a very active program—as our report to the Committee describes—in many areas of the wide spectrum of energy vulnerabilities—going all the way from weather incidents in peacetime, terrorism, and getting into crisis. We had to consider what happened when the *Stark* was hit and the *Roberts* was mined and if Hormuz may close, going into international situations that could affect our country. And then, also, paying a lot of attention to our readiness and preparedness to defend the country in times of war, and the role of energy in mobilization and in wartime.

Consequently, speaking for that and speaking for the NSC's activities, the National Security Council's support of this in the past, I think we had a pretty good system. It remains to be seen how that system will be—you know, what will happen in a new Administration, but we think we have something good to build on.

Senator **Lieberman**. Do you think that Congress will formalize that responsibility and locate it by statute in the NSC?

Mr. **Badolato**. I would not really want to get into that, Mr. Chairman, because I have known General Scowcroft for a lot of years, and he might not appreciate me getting in and playing with his chickens.

Senator **Lieberman**. I understand. Maybe we should consider that a rhetorical question by me.

Mr. **Badolato**. Yes, sir.

Senator **Lieberman**. Again, I appreciate your testimony. This concludes the hearings, and we look forward to keeping in touch with you about the important matters that you have been involved in.

Thank you very much.

Mr. **Badolato**. Thank you, sir.

[Whereupon, at 11:58 a.m., the Committee adjourned subject to the call of the Chair.]

APPENDIX

STATEMENT OF CHARLES C. LANE, STAFF INVESTIGATOR, COMMITTEE ON GOVERNMENTAL AFFAIRS

Mr. Chairman and members of the Committee: My name is Chuck Lane. I have been a special agent with the United States Secret Service for seventeen years. That career has included assignments in intelligence, in security, and in investigations. In February 1988, I was detailed to the Committee on Governmental Affairs. All of the activity in which I have been involved since that date has been associated exclusively with the Committee, and is in no way affiliated with the mission, nor the organization of the United States Secret Service.

In February 1988, the Committee on Governmental Affairs initiated a fact-finding investigation to determine whether energy distribution and telecommunications networks were unnecessarily vulnerable to man-made disruptions, and if so, to identify federal and private initiatives designed to mitigate those vulnerabilities. The investigation attempted to identify (1) the level of threat, (2) the actual vulnerabilities within the networks, (3) the consequences of their exploitation, and (4) the organizations within the federal government and private sector which are most directly affected by these issues.

The primary objective of the investigation was to determine whether a terrorist group (perhaps numbering six to twelve, to twenty individuals), using conventional weapons such as plastique explosives, incendiary devices, backhoes, or even software, could significantly disrupt the nation's energy distribution or telecommunications networks in a peacetime environment.

Much of the information gathered by the Committee was obtained from unclassified government documents, industry documents, and other open source materials. It was supplemented with information obtained from more than one hundred interviews conducted with policy makers, managers, analyists, and technical experts, in both the private and public sector. On behalf of the Committee, I would like to express my gratitude to each of those individuals, agencies, and organizations, for their cooperation, and for their candid discussion of issues. It is the Committee's goal, as it is of everyone who contributed to this effort, that the information collected in this process can be used to promote the security and reliability of our energy distribution and telecommunications networks.

Although we recognize that this is a sensitive subject, in the United States the vulnerabilities of our infrastructures have been frequently exposed. If I can direct your attention to the posters to your (right/left), it becomes obvious that the issues which we are about to discuss have already been identified in the media. These are excerpts from press articles which appeared in major media forums during the period of the Committee's review. The first article discusses an April incident involving the arrest of a suspected Japanese Red Army terrorist, and suggests that the whole northeast could be blacked out by a handful of terrorists. The second article describes the serious impact of raids on the electrical grid of El Salvador in May. The third article presents observations following the fire at the Hinsdale, Illinois, telephone switching center, and suggests that significant vulnerabilities exist in the phone system. November produced a fiber-optic cable break, and the fourth article suggests that fiber-optic cable has introduced a new vulnerability concern. Next, advertising promoted a two night examination of utility vulnerability on an evening news program. Sixth, that same month an article appeared describing the vulnerability of the Strategic Petroleum Reserve to terrorist attacks. These article, and others like them, have attempted to provide accurate representations of the complex subject of vulnerabilities. The public is being told vulnerabilities exist. Well-researched and revealing articles have been, and will continue to be published.

Our investigation examined the distribution networks for crude oil and petroleum products, for natural gas, for electric power, and for telecommunications.

The networks reviewed are almost exclusively municipally, cooperatively, or investor owned. The resources to operate, evaluate, and reconstitute the networks are held by the companies involved. As economic enterprises, there are legitimate proprietary concerns which factor heavily into the decisions made by these companies as to what represents adequate investments in security and reliability measures.

The communications and energy systems were selected because they are vitally important to the public welfare, the national economy, and the national defense, but the federal government owns or operates a relatively insignificant portion of either. In a peacetime environment, the federal government has almost no oversight authority relating to the protection of the networks.

The basic fact is that the development of these networks was not a response to a national security need, but rather an economic venture designed to generate profit. Private industry does not plan, build, or protect its facilities with national security considerations in mind. In the United States, guards and fences, if used at all, are employed because of insurance requirements, petty thefts and vandalism, and abuses from disgruntled employees. Except for minimal regulatory oversight, generally as related to pricing and availability of services, the federal government has no input into construction design and location selection for such facilities as central power stations, switching stations, etc., even though under national emergency conditions, the military might be required to secure the facilities. Commercial facilities are simply designed and constructed based on economic considerations.

Each network consists of a vast, nationwide array of highly visible, mostly unprotected physical structures and support facilities. While they appear to be stand alone networks, they are ultimately interdependent. Electric power producers depend on natural gas and petroleum products for generator start-up and primary fuel. Natural gas and petroleum movers need the electric power to operate pipelines. Telecommunications provide remote monitoring and operating capabilities to pumping stations and switching facilities. Communications are also needed for dispatching repair crews, locating needed replacement parts, and establishing alternate supply routes. Telecommunications suppliers, however, must have electric power to provide telecommunications service, and need petroleum products to run back-up generators when electric power sources are lost.

The distinctions between the networks may be less obvious, but are equally important in the final analysis. The electric power distribution network may be the most vital of the energy distribution systems, because all other energy delivery and telecommunications systems depend on electric power. However, the electric power grid is enormous, and a loss of a portion of that grid may have limited impact on the network as a whole. An alternate transmission route might be established in a relatively short period. On the other hand, a major disruption of a natural gas pipeline might be accomplished with far fewer resources, and produce a lengthy and severe impact on a portion of the country because there is no other way to deliver natural gas in quantity. Any risk assessment must consider both the probability of an successful attack, and the consequences of an attack. In general, the telecommunications and the bulk electric power distribution networks provide a significant number of alternate routes to deliver a product or service to a designated area. This is frequently not the case with pipelines.

The threat and the potential adversary

Many officials in government and industry now privately, or openly, acknowledge that terrorist groups are beginning to recognize the vulnerabilities of highly developed, technology dependent networks. In the future, these groups could turn from the more traditional acts of defiance, such as airline hijackings, assassinations, and bombings, toward disruptions of intricate and sophisticated energy and telecommunications networks. Some countries - El Salvador, West Germany, and Japan, to name only a few - have already experienced significant attacks on these networks.

In 1988, Oliver Revelle, Executive Assistant Director for the FBI, told a Senate Subcommittee that, "...it is unrealistic to assume that we have the ability or resources to guarantee protection to our nation's infrastructure industries from every conceivable terrorist attack".

If networks and infrastructures cannot be physically protected, then the capability to detect imminent assaults before they occur becomes increasingly important. Fortunately, the FBI can claim a number of successes in combatting terrorism.

In spite of these successes, however, the continuing but unsuccessful attempt by the U.S. to close its borders to both drug traffic and illegal aliens has demonstrated how easily people and weapons can be smuggled into the country and potential terrorist support networks are in place in the U.S. Even U.S. street gangs could provide the necessary support. Several are known, or suspected, of having hostile foreign connections. For instance, Los Angeles street gangs have been accused of involvement with the Medellin Cartel, and members of the El Rukn gang of Chicago have been convicted of conspiring with the Libyan government.

Because the United States has a tradition of involvement in the global political arena, the possibility always exists that some group or individual will seek revenge or policy influence through the commission of acts of terrorism. Traditionally, the concern for such acts has been associated with international terrorist groups and those groups continue to pose a potential threat. Significant international terrorist groups, on the other hand, have never targeted the infrastructures of the United States, according to analysts interviewed. If such targeting occurred now, some speculate that it would more than likely result from encouragement by a hostile foreign government, such as Libya or Iran.

A domestic terrorist organization may present an equally significant threat. Such groups are generally made up of individuals whose ideology encourages them to defy federal authority. Members can usually move freely about the country and are comfortable operating within its boundries. Moreover, they have a working knowledge of the country, its people, and their dependence on available services, such as electric power and petroleum products. A simple recognition of the consequences suffered as a result of an accidental disruption of such services may be all that is required to launch such an organization on a campaign of destruction and disruption aimed at discrediting the federal government.

Historically, terrorists have selected high profile targets for their symbolic value, and with the intent to kill, or to bargain with human life. This has resulted in the selection of airliners, military facilities, diplomatic facilities, and other frequently selected targets.

The potential threat, however, cannot be dismissed. If targets are selected for their true value, either to cripple a nation's economy, or as an act of defiance or revenge, these networks present tempting targets. The networks are exposed; they are vulnerable; chances of a successful attack are highly probable;

and significant economic damage might be inflicted as a result. For these reasons it is apparent that a serious effort must be made to understand what impact terrorist attacks could have on these networks, to identify and initiate measures to "harden" networks to withstand assaults, and to make plans to recover services lost as a result of successful attacks. This conclusion is based on the simple recognition that the threat level changes much more rapidly than the vulnerability level. The tragic destruction of the Pan Am airliner in December 1988 provided brutal notice to this fact.

Although intelligence analysts generally agree that there is no current evidence of the targeting of U.S. infrastructures by terrorist groups, the same conclusion does not apply to "special operations" groups. There is reason to be concerned with the protection of the country's infrastructure, including the electric and pipeline grids, in the event of escalating hostilities with the Soviet Union, or some other significant power in the decades to come. This investigation, however, did not directly address the "special operations" threat.

The vulnerability of networks

By their physical nature, networks provide an inexhaustible number of potential targets. Physically protecting a network against any and all possible disruptions is economically impossible. There are hundreds of thousands of miles on interstate pipelines and electric power distribution lines, and endless number of microwave towers, switching stations, and other support facilities. Vulnerabilities are accepted as inherent in such vast networks, and companies are prepared to respond and repair damages, often with a minimum of disruption and inconvenience to the public. In fact, the dropping of support towers and wires and other acts of vandalism and destruction generally create far less damage than earthquakes and hurricanes, and are handled in the normal course of business. Companies have established exemplary records on which to document their response and repair capabilities and mutual assistance and teamwork have been hallmarks of the industries.

A. Critical Nodes

Given the inherent vulnerability in these networks, the question as to whether they are unnecessarily susceptible to extended disruption by sabotage or terrorist action, can only be answered by determining (1) what critical nodes or choke points exist; (2) whether these have been afforded appropriate attention; and (3) whether system redundancies and recovery planning exists in the event of a successful attack.

The Canadian government has codified this approach in the development of a Vital Points Program. The program identifies a vital point as "a resource or facility which is considered essential to the security and continued efficient function of the country or the province/territory, and which therefore warrants extra security precautions to protect it from interference, destruction, or disclosure". The significance of a vital point is then determined by applying the following factors:

* the importance of the service or product it provides or produces

* the dependence of the population or industry on the product

* the cost of replacement

* the replacement time, and

* the availability of substitutes

The United States does not have such a centralized, defined program.

Opinions differ as to whether the federal government has a need, or right, to know where specific critical nodes exist within a network. The electric power industry feels strongly that it does not. The Department of Energy has currently taken the position that there is no need to establish a national list of critical nodes which would be held by one or more federal agencies. The Department of Defense, on the other hand, feels that it is necessary to identify and establish a list of critical nodes vital to defense related industries and installations within each Army district in the U.S.

Systems are constructed differently, and critical nodes may vary. Generically speaking, critical nodes could include pump stations on liquid pipelines, compressor stations on natural gas pipelines, extra high voltage transformers and substations in the electric transmission system, control centers, switching centers in the telecommunications networks, or even portions of transmission or distribution routes. In most cases the reconstruction of a critical node involves the replacement of expensive, custom-designed, long-lead-time components which require a significant, and currently deteriorating, manufacturing base. Critical nodes are rarely afforded any more protection than any other node in the system; and in some instances the loss of one, or a multiple of similar nodes, may create a situation in which the populace of a city, state, or a larger geographic region could be generally denied the service or product provided by the system for days, weeks, or longer. Fortunately, most of our systems are robust - - without real expertise in choosing targets, the impact of even a serious attack may not be catastrophic in an national security emergency preparedness sense, but the results could have a profound effect on a community.

Although our investigation focused primarily on long distance distribution systems, any major metropolitan area has the same problem. Most have a relativley small number of critical nodes supporting a service such as phone, electric power, or petroleum and gas supply. Though it may be of limited duration, a major portion of any metropolitan area will be denied a service by eliminating those nodes. In some scenarios a portion of the disruption might continue for several days, weeks or months.

B. Industry practices

To heighten our concerns, there are several standard operating practices observed in industry which increase vulnerability concerns. Examples include:

1. The storage of spare units next to operating units.

2. The operation of pipelines from a single control center, with no alternate control center available.

3. The concentration of high volume switches in a single structure.

4. The installation of expensive, essential equipment in a facility protected by little more than a fence.

C. Physical Security

Does poor physical security contribute to vulnerability concerns? That question is difficult to answer. In some cases, increased physical security measures appear to be a simple solution to the problem of exposed facilities; in other cases, it may be the least productive and most expensive approach to ensuring that service is maintained. In 1979, the Government Accounting Office issued a report entitled Key Crude Oil and Product Pipelines are Vulnerable to Disruptions. That report documented instances of unlocked doors and gates at key facilities, loose or non-existent key and pass control systems, and generally poor physical security planning associated with a number of key pipelines. Many of those conditions still exist. Two operators of major pipelines responded to the 1979 GAO report asserting that even a highly sophisticated physical security program would not succeed in eliminating vulnerabilities in the pipelines. Other industries share this attitude.

D. Public information

Ironically, both government and industry, responding to other legitimate policy concerns and operational necessities, have made the job easier for a potential adversary. For instance, the 100th Congress, passed legislation, which in the interest of public safety, requires pipeline operators to provide detailed maps of their systems to state and local governments, to allow for emergency planning and public safety education. Environmental impact studies, as well as reports accumulated by DOE, FERC, FCC, and Transportation often contained detailed information and are available to the public. Relatively detailed maps of the various pipelines systems and the electrical power grids can also be purchased from the industries themselves. It is undesirable and impossible to reverse these policies. However, such policies do increase vulnerabilities by making vital information available.

Coincidently, a GAO report released in December 1988 documented the use of material obtained from a library by a mock "terrorist" team during an assault on the SPR in 1987.

E. Complexity

There are also a number of complex forces which have crept into the present industrial environment. The potential impact of any one of these forces on recovery efforts is difficult to assess, but in the final analysis, each must be given its due consideration. For example:

1. A media article recently reported that most businesses are ill-prepared to cope with electronic disasters as computers have crept gradually into companies, and many top executives are unaware of their strategic importance. The same article quoted a recent University of Texas study which found that 75 percent of the businesses surveyed would have a critical or total loss of functioning within fourteen days if they lost their computer support. More than 85 percent of the companies surveyed indicated they were totally or heavily dependent on their computer facilities. That dependency is also evident in the energy and telecommunications networks.

2. There are an increasing number of telecommunications resources within the private sector of the economy, exclusive of the public carriers. Some, such as the broadcast industry, are active in telecommunications national emergency preparedness planning. Others, like the railroads and pipelines systems, are not. The potential vulnerability of these private systems may exceed that associated with the use of public systems. The strengths or vulnerabilities created within the national telecommunications structure by the growing emergence of these private systems are not fully known at this time.

3. Both the telecommunications and the heavy manufacturing industries in the U.S. have decreased significantly. This forces a dependence on foreign sources. This trend has resulted in the loss of skilled personnel as well as production facilities.

4. Lack of standardization is typical of a free enterprise utility system, and generally creates a healthy, competitive environment. However, it has the potential of becoming a handicap in the event of mass destruction, where the reconstruction of the

system depends upon availability of spare parts from unaffected areas. Lack of standardization discourages stockpiling.

5. An increasingly popular management philosophy in telecommunications and heavy manufacturing industries, if not most businesses, is to reduce inventories to the absolute minimum level possible. The American Production and Inventory Control Society identifies this "Just-In-Time" management philosophy as "... the movement of material at the necessary place, at the necessary time". However, Just-In-Time management involves some very clearly defined concepts. Industry in general, however, has adopted a number of variations of this approach, some of which may only involve a reduction of inventories. Further, it is important to recognize that while Just-In-Time management may have a useful application in the manufacturing process, it is not applicable to the stockpiling of critical replacement items, nor should it be confused with the practice of using industrial items, such as transformers, beyond the maximum limits of their life expectancy and replacing the items only when absolutely necessary.

6. When a telecommunications or energy service or product is disrupted, the order of service restoration and the allocation of available supply could become important considerations. Both state and federal regulations may have application. State regulations generally attempt to protect the individual citizen and may not serve the more complex interests of the federal government, such as failing to provide priority service to a critical defense facility.

7. In some instances, conflict of interests or antitrust concerns, and/or increased competition among competing vendors may have some undesirable effects on efforts to develop reliable systems or recovery programs.

The consequences of disruptions

Accidents and natural disasters have provided more than an adequate indication of the potential consequences of mass disruptions of crucial systems. Several incidents which have occurred in recent years have demonstrated the reliance of the American public on these networks and the potential catastrophe associated with their destruction.

The first to come to mind are the massive electrical outages which occurred in New England in 1965, and in New York again in 1977. But less spectacular events have occurred in recent months.

A major refinery exploded and burned in Louisana in May 1988. Fortunately, due to the early morning hour in which the explosions occurred, fewer than 100 of the 1600 employees were on duty. At the time, repair costs from the fire were estimated as high as $100 million.

On May 8, 1988, a fire destroyed a high-volume telephone switching station at an Illinois Bell facility in Hinsdale, Illinois. In September, another fire in an electric vault in Seattle instantly put a fifty-square block area of the city in darkness for several days.

On November 18, 1988, a major fiber-optic communications line of AT&T was accidently severed by a construction crew in New Jersey. While none of these disruptions were the result of terrorist activity or sabotage, they serve notice that isolated incidents can create major disruptions. In isolated cases, help and expertise can be brought in from unaffected areas. However, if terrorists were to target such systems and achieve significant destruction at multiple sites, the impact of such disruptions could have a dramatic and catastrophic impact on the public welfare, and on the local, regional, or national economy.

In isolated cases, help and expertise can be brought in from unaffected area. However, if terrorists were to target such systems and achieve significant destruction at multiple sites, the impact of such disruptions could have a dramatic and catastrophic impact on the public welfare, and on the local, regional, or national economy.

For instance, a loss of a major petroleum pipeline could send gasoline prices sky-rocketing; require localized rationing; and require herculean efforts to find alternative transport for supplies. The loss of electric power in a major area has already been demonstrated with regard to its impact on society; and if a natural gas pipeline is lost, there is no other mode of transportation available. Under the worst of conditions, an extended disruption could interrupt local service and require pilot lights to be relighted.

Government and industry interaction

The federal government has the responsibility of maintaining a defense capability and protecting the welfare of the public. Since the energy and telecommunications networks are vital to that effort, the federal government must be able to effectively work through private industry to achieve those objectives. Opinions differ as to what constitutes an adequate commitment of resources and an acceptable level of risks. In many ways the vital question of who is going to pay to mitigate the risks dictates the ambiguity of responses.

The approaches used by the federal government in addressing energy and telecommunications concerns, vary in several significant respects. The National Communications System, with approximatley 100 employees and an annual budget of approximately $75 million dollars, works closely with a committee appointed by the President called the National Security Telecommunications Advisory Committee (NSTAC). This committee consists of executives representing the top thirty telecommunications providers in the nation. Under the Committee's direction, industry task forces continually identify and research potential problems, and work with the NCS to correct them. In addition, it is the intention of the federal government to supplement the physical assets of the public switched network. Energy issues are addressed by the Office of Energy Emergencies with 71 employees and an annual budget of $6.2 million. The energy effort is not assisted by anything equivalent to NSTAC. The Department of Energy attempts to reduce vulnerabilities through outreach programs, involving studies, awareness programs, and exercises involving simulated disruptions. A more detailed discussion follows.

National Security Emergency Preparedness

Actions taken by the federal government since 1982 have demonstrated an aggressive approach to NSEP planning. The key instrument in this effort has been the National Security Council. Current direction and responsibilities for NSEP planning are defined in E.O. 12656, issued November 18, 1988, which replaced former E.O. 11490. This revision established the National Security Council as the principal forum for consideration of national security emergency preparedness policy, and shifted the responsibility for protecting facilities and resources essential to the national defense and national welfare to the cognizant federal department or agency. The Federal Emergency Management Agency (FEMA), which previously held this protection responsibility for all assets under E.O. 10421 (which was recinded) and E.O. 12148, will serve as a coordinator and advisory agency. Telecommunications NSEP policy, excluded from E.O. 11490 and E.O. 12656, is based on E.O. 12472 issued April 3, 1984, but is consistent with the approach defined in E.O. 12656.

In September 1985, the NSC created a Senior Interagency Group on National Security Emergency Preparedness (SIG-NSEP). SIG-NSEP is chaired by the Assistant to the President for National Security Affairs and includes representatives from the Departments of Justice, Defense, Treasury, and the Office of Management and Budget. The Director of FEMA was designated an advisor to this group.

In April 1986, SIG-NSEP created inter-agency groups (IGs) to focus on policy issues in (1) civil defense, (2) national mobilization, and (3) energy vulnerability. The Committee of Principals of the National Communications System was designated the fourth IG to focus on telecommunications. The energy group was designated the Interagency Group On Energy Vulnerability, chaired by DOE.

Telecommunications

The National Communications System (NCS) is an interagency activity with National Security Emergency Preparedness responsibilities across the full spectrum of crisis and emergencies--from natural disasters and man-made crisis through conventional and nuclear war. NCS is an independent organization, with approximately 100 employees, but is co-located with the Defense Communications Agency. The Manager, NCS, is also the Director of the Defense Communications Agency. Often their activities appear to be inseparable. The NCS, however, was created to "provide the necessary communications for the federal government under all conditions ..." NSDD 201 requires each of the member federal departments and agencies to contribute to the funding of NCS, but DOD accounts for the majority of the total budget. NCS responsibilities include planning for and implementation of enhancements to the national telecommunications infrastructure, and ensuring that mechanisms exist for the management and use of national telecommunications resources in support of non-wartime and war time emergencies.

The Committee of Principals (COP) of the NCS, consisting of representatives of 23 federal agencies, was established by E.O. 12472, and collectively represents the aggregrate NSEP needs of the Federal government. COP is responsible for the development and consideration of NSEP telecommunications programs and activities, and in 1986 was designated one of the four IG groups under SIG-NSEP with responsibility for telecommunications planning. COP then established the Council of Representatives as a permanent subordinate body. Goals of the NCS are set in accordance with E.O. 12472 (Assignment of National Security and Emergency Preparedness Telecommunications Functions), and NSDD 97 (National Security Telecommunications Policy).

The Federal Communications Agency (FCC) is an independent regulatory agency. One of its prime responsibilities with regard to telecommunications disruptions, is its authority to designate NSEP restoration priorities. In late 1988, the FCC issued a comprehensive guide for telephone service restoration priority at all levels of service, i.e. for operating companies and long distance carriers. This policy issuance resulted from efforts by the NSTAC and NCS. Several important responsibilities associated with programs conducted by the National Communications System are delegated to NCS from FCC authorities.

In view of the fact that the federal government is heavily dependent upon the commercial sector for 95 percent of its telecommunications services, including satisfaction of critical NSEP telecommunications requirements, former President Reagan established the National Security Telecommunications Advisory Committee (NSTAC) in 1982 by E.O. 12382, and renewed its charter for the third time in 1987. The NSTAC, currently representing 30 member companies, provides advice and assistance to the Government from the perspective of the telecommunications industry for improving NSEP telecommunications capabilities. NSTAC then formed working groups and ad hoc task forces to identify and explore concerns within that industry. Industry funds many of the associated costs.

Energy

The Department of Energy currently has a program attempting to deal with concerns for vulnerabilities in the nation's energy supply networks. Responsibility for this program belongs to the Office of the Deputy Assistant Secretary for Energy Emergencies (OEE), located under the Office of the Assistant Secretary for International Affairs and Energy Emergencies.

OEE has an authorized personnel level of 71 full time employees and an operating budget of $6.2 million per year. Personnel and budget have remained approximately the same since 1982. It is significant that of the budget, only about $800,000 is not committed to salary costs.

The Office of Energy Emergencies is charged with the following responsibilities:

direct energy emergency preparedness planning and programs;

develop and promote energy security policy and programs;

direct energy emergency operations;

direct international energy emergency policy and programs;

and, coordinate and direct DOE's continuity of government program.

The National Defense Executive Reserve (NDER) is a voluntary assembly of executives and operating managers recruited from the various industries. Approximately eight federal departments currently have NDER programs. In a time of declared national emergency this reserve is responsible for assisting federal authorities in setting distribution and allocation priorities, and coordinating industry efforts to meet national needs and restoration efforts. However, lacking an industry executive committee, DOE uses this body to identify and address a number of issues.

The North American Electric Reliability (NERC) collectively represents the 3500 electrical systems in the U.S. In 1984, NERC worked with security officials concerned with the possibility of a terrorist disruption of electric power during the Los Angeles Olympics. In January 1987, NERC formed the National Electric Security Committee, to work in conjunction with the NSC and DOE to address concerns in the electric power industry.

The National Petroleum Council (NPC) was formed in 1946 and still exists. This federally chartered, privately funded advisory committee has 121 members selected and appointed by the Secretary of Energy. Members serve as representatives of their industry and associated interests as a whole, and not as representatives of their particular companies. The NPC has prepared over 200 reports dealing with every aspect of oil and gas operations. The costs associated with the research and preparation of some of these reports is estimated at more than one million dollars.

The Office of Pipeline Safety is a small organization under the Research and Special Programs Administration of DOT. This office attempts to identify and address issues of public safety associated with natural gas and hazardous liquid pipeline systems. Regulations and enforcement authority are prescribed in the Code of Federal Regulations, Title 49-Transportation, Parts 190-195. Enforcement of pipeline safety standards is the responsibility of 20 federal field inspectors working closely with various state agencies with similar responsibilities. This office is not concerned with the physical protection of the pipeline systems, but certain safety regulations do in fact require fencing of facilties such as pump stations.

Defense

Since most federal initiatives directed at guaranteeing adequate energy and telecommunications assets are related to national defense concerns, the Department of Defense (DOD), through a variety of agencies and programs, has been a key player. Under defense plans for the protection of the continental United States (CONUS), the Department of Defense has the responsibility of protecting designated key assets. DOD, of course, has had absolutely no input into the design or planning of these assets, and no national data base to rely upon.

E.O. 10421, issued in 1952, required federal agencies to develop and execute programs and measures for the physical security of designated facilities important to national mobilization, under the auspices of the National Security Resources Board. Within DOD, Department of Defense Directive 5160.54 implemented the requirements of the original E.O. 10421 and established a Key Facilities Program. Critical defense related industrial and manufacturing facilities in the private sector were placed on a classified Key Facilities List. Facilities placed on this list were sponsored by a component of the armed forces, and the owner/operator voluntarily accepted the designation and associated responsibilities, including a requirement to allow the Defense Investigative Service to conduct on-site physical security surveys.

During the period 1982-83, DOD began to look at both the essential facilities and the supporting energy base for the operation of the facilities. In 1983, Defense Energy Memorandum 83-1 established energy supply assurance as its highest priority for the first time. This has resulted in an effort to establish a list of key facilities together with a list of critical support systems, such as energy distribution systems, to be incorporated into the basic planning for the land defense of CONUS. Changed from the Key Facilities Program to the Key Assets Protection Program (KAPP) with a classified Key Assets List (KAL), this facilities identification and protection program was given new life in 1983. KAPP is currently based on DOD Directive No. 5160.54, dated December 5, 1986. A classified KAL identifies those facilities which will be protected under a program requiring national guard or state reserve units, acting under the direction of a state area command (STARC), to protect designated facilities while mobilizing for future commitment.

Law enforcement

The Federal Bureau of Investigation is the lead agency for counterterrorism in the United States.

In 1982, the FBI established a counter-terrorism program on the same level with programs addressing white collar crime, foreign counter-intelligence and organized crime. Mr. Revelle's recent Senate testimony identified 54 potential terrorist incidents prevented since 1982 through the collection of intelligence and other actions. In fact, FBI reports show a decline in terrorist incidents in the U.S. since 1980.

In 1983, the FBI received new jurisdiction dealing with destruction of energy facilities with the enactment of 18 USC 1366. In conjunction with the Comprehensive Crime Control Act of 1984 and the Diplomatic Security and Anti-Terrorism Act of 1986, the FBI now has more jurisdiction than ever in history to deal with terrorist groups or members and destruction of energy facilities.

In addition, the FBI, through the Department of Justice, has been officially tasked with the development of an infrastructure protection program, by E.O. 12656, Part 11, Sec. 1102 (1). One FBI initiative known to be under study is the development of a domestic terrorist threat warning system.

Conclusion

In summary, this investigation concluded that the networks of the United States are vulnerable to multi-site terrorist attacks. That is, targets are likely to be destroyed. However, the redundancy built into the networks make them very dependable, and the real question is what level of services would be lost from such an attack. In many cases, the consequences appear to be manageable; in a few cases, the consequences are potentially catastrophic.

Even though the industries have demonstrated a tremendous capability to respond to emergencies over the years, some new variables are introduced in a terrorist scenario. First, there may be multi-site destruction which destroys assets or capabilities normally available in a recovery effort. For instance, a redundant route or a by-pass capability may be destroyed in a multi-site incident. Second, the stockpile of replacement components or even whole pieces of equipment, perfectly adequate under normal operating conditions, may be inadequate in a terrorist scenario. For instance, spare pumps or extra-high-voltage power transformers, pre-positioned with the operating units to ensure a back-up capability, may also be destroyed.

Most industry officials believe that prevention of intentional disruptions by dedicated individuals is impossible, and that it is more economical and practical to devote resources to other approaches, such as establishing redundant routes or planning for recoveries. Most efforts to date have either been directed at providing a survivable industrial base to support a war-time effort and recovery program, or at the opposite end of the spectrum dealing with public safety, theft, and vandalism. Many officials within industry are not convinced that a serious terrorist threat really exists.

Beyond the more clearly drawn NSEP reponsibilities of federal government agencies, there is a vacuum in the current authority, planning, and ability to impose requirements to ensure a service capability to the public. Most authorities and responsibilities are addressed only to NSEP considerations. While some NSEP programs provide some measure of protection to the public in non-declared emergencies, there are no programs designed specifically to ensure the public a minimal level of service, and there can be serious consequences when that service capability is lost, as we will hear next regarding the Hinsdale fire.

Mr. Chairman, there are some very complicated issue to be explored regarding vulnerabilities and reliability of services. I hope this overview assists the Committee in its review.

Thank you.

TESTIMONY

OF

N. RICHARD KING
EXECUTIVE DIRECTOR
ILLINOIS COMMERCE COMMISSION

BEFORE THE
UNITED STATES SENATE
COMMITTEE ON GOVERNMENTAL AFFAIRS

ON BEHALF OF
THE HONORABLE JAMES R. THOMPSON
GOVERNOR OF THE STATE OF ILLINOIS

FEBRUARY 7, 1989

TABLE OF CONTENTS

INTRODUCTION.. 1

I. BACKGROUND.. 4

A. OVERVIEW OF STATE AGENCIES AND DEPARTMENTS....... 4

B. THE HINSDALE CENTRAL OFFICE (HCO)................ 6

C. HISTORY OF FIRES AT CENTRAL OFFICES..............14

II. THE MAY 8, 1988, FIRE................................18

A. FACTS SURROUNDING THE FIRE........................18

B. THE IMPACT OF THE FIRE............................22

C. THE RESTORAL OF THE NETWORK......................33

III. REMEDIAL EFFORTS OF STATE AGENCIES TO DATE 39

CONCLUSION..44

ATTACHMENTS

Attachment 1 - Current Switching System

Attachment 2 - Previous Copper Switching System

Attachment 3 - Fire Investigation's Organizational Chart

Attachment 4 - Interim Report Issued

INTRODUCTION

On May 8, 1988, a fire occurred at the Hinsdale Central Office (HCO) of Illinois Bell Telephone Company. That fire is now identified as the most serious fire ever encountered by that company and by the telephone industry as a whole. The fire disrupted local and long-distance communications over a large area, including communications vital to the provision of emergency services.

The State of Illinois shares the concerns of this Committee. It is necessary and appropriate for the government, both federal and state, to assess the potential consequences of major disruptions in telecommunications' capabilities and to assess the adequacy of both private and governmental programs designed to prevent, or to respond to, such emergencies.

The State of Illinois initiated its own efforts to address these concerns soon after the Hinsdale fire occurred. Within days of the fire, the Office of the State Fire Marshal engaged outside consulting engineers to assist in the investigation of the fire. On May 10, 1988, the Staff of the Illinois Commerce Commission made its first on-site inspection of the fire damage. Several days later, the ICC Staff initiated its own investigation into the cause and origin of the fire with a view toward recommendations to enhance fire prevention and protection and to reduce network vulnerability to any future, similar occurrence. The staff secured an agreement from Illinois Bell to fund the services of an independent engineering consulting firm to serve at the exclusive direction of the Commission. The Commission staff retained the services of Forensic Technologies International Corporation (FTI), Annapolis, Maryland, a nationally recognized consulting engineering firm specializing in fire and failure analyses, to conduct an in-depth investigation into the cause and origin of the fire and to make specific loss prevention recommendations (Attachment 5).

In addition, the Illinois Commerce Commission, at the request of Neil F. Hartigan, the State's Attorney General, instituted a public on-the-record investigation of the fire. The purposes of this investigation were to inquire into the adequacy of Illinois Bell's provision of telecommunications services; to consider adopting emergency plans for catastrophic incidents, including emergency alternative services; and to assess the extent of damages caused by the fire.

Both of these investigations are currently in progress. A final joint report of the Office of State Fire Marshal and the Illinois Commerce Commission staff, as prepared by FTI, assessing the cause and origin of the fire as well as providing recommendations for preventive measures is expected by February

28, 1989. A copy of that report will be made available to this Committee. While we are unable at this time to provide this Committee with any of the conclusions and recommendations which will be contained in the final report, we can and do provide the basic facts surrounding the incident.

This testimony is organized into three sections. The first section presents an overview of the state agencies and departments responsible for coordinating the governmental response to incidents such as the Hinsdale fire (Attachment 5), some background information on the Hinsdale Central Office and on Bell's network configuration (Attachments 1 and 2), and the history of major fires at central offices. In the second section, the specifics of the May 8 fire are presented. This section includes the facts surrounding the fire, the impact of the fire, and the efforts by various governmental agencies and Illinois Bell to respond to the emergency and to restore service. The final section addresses the actions which are currently being undertaken by the State of Illinois to limit or prevent the consequences of future disruptions to telecommunications capabilities (Attachment 3).

I.

BACKGROUND

A. OVERVIEW OF STATE AGENCIES AND DEPARTMENTS

Illinois Emergency Services and Disaster Agency

The State of Illinois' concern for emergency preparedness in the event of natural or other disaster, including fire, long pre-dated the May 8, 1988, Hinsdale Central Office fire. In 1975, the General Assembly passed the Illinois Emergency Services and Disaster Agency Act of 1975. This Act created the Illinois Emergency Services and Disaster Agency and charged it with responsibility for coordinating and implementing programs for disaster prevention, preparedness, response and recovery. The agency coordinates its activities with those of the federal government, local governmental units and public and private agencies.

Office of the State Fire Marshal

By law, the fire chief of every municipal fire department or fire protection district investigates the cause, origin, and circumstances of fire within the department's jurisdiction. The

Office of the State Fire Marshal (OSFM) is charged with supervising and directing any such investigation where circumstances warrant. In addition, the OSFM promulgates rules for fire prevention and protection, and administers the Illinois Fire Protection Training Act.

Illinois Commerce Commission

The Illinois Commerce Commission (I.C.C.) is responsible for the economic and safety regulation of gas, electric, telephone, water and sewer public utilities; intra-state motor carriers, railroad and pipeline safety; and towing companies. With regard to the general supervision of telecommunications carriers in Illinois, the I.C.C. is responsible for the manner in which their plant, equipment, and other property are operated and maintained. The Commission promulgates rules for the safe operation of telephone plant and equipment to promote and safeguard the health and safety of the public, customers, and employees.

The Commission has specific authority to investigate all accidents occurring on telephone company property and to report the consequences of such accidents to customers and the public. The Commission's oversight responsibilities are carried out by the Illinois Commerce Commission staff under the direction of the Executive Director.

All three state agencies have played important, closely coordinated roles in monitoring service restoration after the Hinsdale fire, investigating the cause and origin, and are preparing recommendations for enhancing fire prevention and protection in telephone company central offices.

B. THE HINSDALE CENTRAL OFFICE (HCO)

In general, telephone company central offices are switching centers for local and toll equipment. There are over 11,500 central offices in the United States. In addition, there are approximately 9,000 transmission stations located along major transmission lines around the nation. Central offices exist in a wide variety of configurations. Some are as small as 400 square feet, while others occupy over one million square feet. Many rural central offices are single story, while urban central offices can be high rise construction.

The evolution of the modern central office building began in the 1920s with the advent of semi-automatic switching equipment. By 1930, fully automatic switching equipment was beginning to replace the manual and semi-automatic equipment. Until the introduction of the Electronic Switching System (ESS) in 1965, all central offices included space for operators to work near the switching equipment. By the 1970s ESS's had begun to replace older equipment. Between the 1920s and early 1970s, central offices were staffed with up to 500 personnel who operated and performed maintenance on the switching equipment.

The ESS created a revolution in central office technology -- not only in switching technology, but also in building design and operating and maintenance procedures. The ESS, introduced in 1965, was not only fully automatic but was also self-diagnostic. The equipment was also able to make minor repairs on itself and to automatically disconnect from the system in the event of a major failure. The ESS self-diagnostic information could also be transmitted to remote locations. The ESS had two major effects on central office technology. First, the operators could be housed in standard office space which was less costly than the central offices built to conform to the equipment requirements. Secondly, the central offices no longer required technicians to continuously staff them. For the past 20 years, new central offices have been designed primarily for equipment.

In order to accommodate growing customer demand, to meet customers' high-speed data transmission needs and to take advantage of the maintenance and transmission cost savings of fiber optics, the telephone industry decided in the early 1980s to replace its existing copper cable telephone network with a fiber optic network for connecting its switching centers.

Cable-for-cable replacement of copper with fiber would have been a costly and inefficient process taking several years. The copper cable network was designed as a "mesh," or "grid," with switching centers in metropolitan areas usually connected directly to several other centers.

The increased capacity of fiber optic systems -- and the ability of those systems to handle heavy volumes of customer calls -- meant that more traffic could be carried over fewer routes.

This technology made it possible to exceed the capability of the copper network by restructuring the network, i.e., by connecting switching centers via a central "hub" center, rather than by recreating the grid network of switching centers connected directly to each other. (See Attachment 1)

These hub centers function much like large airports such as O'Hare in that traffic from smaller surrounding switching centers passes through the hub to connect the smaller centers with one another. This is similar to the way smaller "feeder" airports route passengers through large airports, then on to other destinations.

On the old copper network, a call from Aurora, Illinois to Oak Park, Illinois might have traveled on a direct route from Aurora to Naperville, then on a route from Naperville to Lombard, and finally on a third route from Lombard to Oak Park.

On the new fiber network, the call from Aurora is routed via one path to Hinsdale, then relayed over another path to Oak Park. As a result of this architecture, the 40 switching centers connected to Hinsdale have access to one another, but without the expense of building direct paths between several central offices (Attachment 2).

Although the term "fiber hub" is new, the hub concept of carrying telecommunications is almost as old as the telecommunications industry itself.

Long-distance telecommunications traffic always has been routed to a type of hub. Hubbing also is used when two nearby switching centers have relatively light traffic between them but have heavy calling volume to a third center. The two centers with the lower traffic volume are not connected to each other, but are instead connected via the third center with which they each have a heavier volume of traffic.

There currently are six main, or "gateway," hubs in the Chicago metropolitan area.

The fiber optic hub network offers several service and economic advantages over the old copper cable "mesh" network: greater flexibility to meet increasingly sophisticated customer demands, greater capacity, simpler and easier administration of network routing, reduced maintenance, and establishment of a framework or architecture for implementing future advances in fiber optic technology.

An article in the April 1988 issue of Bellcore's Exchange magazine states: "...The key to optimum fiber network design is fiber hubbing. The basic idea is this: If it costs very little to transmit a long way and if the capacity available along each route is very large, then traffic can be sent from various sources to a building selected to serve as a common hub. At that hub, a high-speed digital cross-connect system can be used to sort traffic and route it to various destinations."

The Hinsdale wire center is the major, or gateway, hub for the high-traffic west and southwest suburban Chicago communications center of the phone system. (See Attachment 2). On May 8, 1988, the facility housed an electronic switching machine (1AESS) used to provide local exchange service to approximately 38,000 customers on over 42,000 lines in the communities of Hinsdale, Clarendon Hills, and Willowbrook and parts of Burr Ridge, Darien, Oak Brook, and Westmont, as well as unincorporated areas in south DuPage County, Illinois. The local exchange switch permitted these customers to make and receive local and long-distance calls.

The Hinsdale facility also housed network transmission equipment and was a gateway office for Illinois Bell's fiber optic network. Nearly all interoffice calls (calls that originate in one central office and terminate in another) between more than 40 Illinois Bell central offices and other points in Illinois Bell's network or the long distance network passed through the Hinsdale fiber optic transmission equipment.

In all, about 3.5 million calls per day originated, terminated or were routed through the Hinsdale facility.

The Hinsdale facility also housed equipment which was used to provide special services, that is, circuits which were dedicated to particular customers. These circuits were used for various purposes such as data transmission, alarm circuits, and private links.

Numerous equipment functions at the Hinsdale facility are continually monitored. The temperature, humidity, boiler loss, power loss, and sump pump are monitored by direct digital control which is designated as the Building Equipment Status Indicating System (BESIS). BESIS is located in Chicago. There are approximately thirty functions which are continually monitored. The system takes about forty seconds to scan all monitored functions. The data are relayed to a CRT screen and also printed out. Changes to these environmental controls can be performed remotely.

At the time of the fire, the fire alarms were not connected or transmitted to BESIS. The equipment and fire alarm systems are monitored by an Illinois Bell Telephone central office technician in Springfield, Illinois, in the Division Alarm Reporting Center (DARC). The alarm system functions to alert the Springfield facility of telecommunications equipment malfunctions and fires in the building, but does not provide a specific location of the failed equipment.

The building was equipped with an ionization smoke detection system designed to detect products of combustion released during an incipient fire situation. In the early stages of a fire, smoke products (both visible and invisible) are normally released into an area before any appreciable heat is released. The system that was installed, and that was operational, was an early warning, product-of-combustion detection system. Additionally, there were smoke detectors installed in the ducts of the air circulating system. These detectors were designed to detect the presence of smoke and to shut off the air supply system in order to prevent smoke from being distributed throughout the building. In rooms not involved in the fire, there were different types of detectors, such as an infrared flame detector in the diesel generator room and heat detectors in other rooms. Upon detection of products of combustion, the system was designed to perform the following actions:

- Sound an alarm in the building.

- Illuminate a lamp indicating the zone of alarm initiation on an enunciator board near the front entrance of the building. A building layout diagram was located on the enunciator to aid in determining the location of the alarm.

- Transmit a signal to an Illinois Bell facility (DARC) located in Springfield, Illinois.

- Shut down the building air circulating fan system.

There are two diesel-powered generators located in the basement stand-by generator room which are monitored by DARC. These generators are normally off until incoming electrical power is lost from the local electric utility company. These generators are provided with fuel from two diesel tanks which are located adjacent to the generators. In the event of a utility power failure, the generators are able to operate under full load for approximately four hours with this fuel supply. Additional fuel could be trucked in to replenish the tanks in the event of a long term power failure. Two banks of batteries located in the southeast corner of the basement constantly supply DC power to the communications equipment system, insuring that variations in or loss of the utility power source do not cause problems in the communications equipment. AC power for emergency equipment is supplied by a DC to AC inverter.

C. HISTORY OF FIRES AT CENTRAL OFFICES

Prior to the Hinsdale fire, only two other major fires have occurred at central offices. The first central office fire occurred at the New York Telephone Company's (NYT) main switching center in New York City. The main switching center was located in an eleven story building with reinforced concrete floors. On February 27, 1975, a fire started in the telecommunications cables in the basement. The fire remained confined because of the configuration and number of walls and partitions. The heat increased in this area to at least 600°C and ignited PVC insulated cables leading from the vault to the upper floors. When an alarm was finally turned in, heavy black smoke made maneuvering on the basement level difficult. At the height of the fire fighting activities, over 300 fire fighters from 50-60 units were working to control the fire. The fire was extinguished about 3 1/2 hours after the alarm was transmitted. However, gases from the PVC cables accumulated in the vault and ignited when the gases came into contact with hot wires in the area. This reignition fire spread rapidly along the PVC cables to the upper floors where fire fighters performing clean-up were injured from the inhalation of noxious gases. This fire resulted in 41,000 subscribers being without service. Emergency service was provided through mobile phone banks and microwave hook-ups.

The second and most recent telephone central office fire occurred on February 18, 1987, at another New York Telephone facility, this one in the Bushwick Central Office in Brooklyn. The fire started in communications equipment on the first floor. One of three employees in the building at the time discovered the fire and contacted the fire department. Approximately 100 fire fighters battled the blaze and no one was injured.

The fire resulted in loss of service to over 41,000 telephone subscribers in six exchanges, ten percent of which were business customers, including local police and fire departments and six hospitals. Emergency communications were provided to these critical services by modifying outgoing lines for incoming service through the use of microwave dishes for line-of-sight communications to another switching center and the use of cellular mobile telephones. Residential areas were provided with over 200 emergency coin telephones, ten roving vans were equipped with cellular phones, and emergency centers were established in police stations. NYT also set up a business message center for businesses in the affected area and hand-delivered the messages.

The fire damaged the 1ESS switch (the predecessor of the 1AESS switch at Hinsdale) which served 28,000 customers and had to be completely cleaned and repaired. A second switch handling 13,000 customers had to be completely replaced, and the entire main distribution frame had to be rebuilt. To restore service as quickly as possible, a command center was established in trailers adjacent to the central office. A DMS-200 switch (normally a long lead time item), which was being installed in a nearby central office, was modified and placed in the Bushwick Central Office, speeding the repair time. Within ten days, 28,000 lines were restored and the remaining 13,000 lines were back in service by March 5.

The two fires described above are the only incidents of major proportion which we have discovered. From this information, it can be observed that central office fires are a fairly rare occurrence.

Within 72 hours of the Hinsdale fire, the staff of the Commission decided that the magnitude of the event required a more comprehensive and intensive investigation than had previously been undertaken anywhere in the country. This added effort was needed to ensure the Commission's public interest mandate was honored.

I believe the multi-disciplined and comprehensive approach, which although time-consuming and thus frustrating to many, will yield a final report that will have a high level of credibility with the telecommunications industry and consumers This belief is supported by the Interim Summary Report submitted by the staff of the Illinois Commerce Commission and the Office of the State Fire Marshal on September 6, 1988. To underscore the thoroughness of the effort, it should be noted that the Interim Report contained a projection that the Final Report would be completed by mid-November 1988; however, subsequent evaluations of the schedule and testing requirements rendered that date overly optimistic (Attachment 4).

II.

THE MAY 8, 1988, FIRE

A. FACTS SURROUNDING THE FIRE

In the late afternoon of May 8, 1988, the Hinsdale fire and power alarms and the equipment alarms for the local exchange switch were being monitored remotely by a technician in Illinois Bell's off hours alarm center in Springfield, Illinois. It has become standard industry practice for central offices to be unattended during non-regular work hours and for alarms to be monitored remotely. The sophistication and reliability of modern electronic telecommunications equipment has greatly reduced the maintenance required. A small number of mobile technicians ("roamers") can easily handle the maintenance work in many central office facilities during off-hour periods. Moreover, the sophistication of alarm technology has allowed numerous offices to be monitored remotely from a central location.

Accordingly, the Hinsdale office was unattended, although technicians had visited the building at times during the day to carry out various work operations.

At the time the fire broke out, a tornado watch was in effect for northeastern Illinois. High winds had been reported in the

Hinsdale area, and several local power interruptions had occurred. A power interruption occurred at the Hinsdale central office at 3:50 p.m. and was reported automatically in the Springfield alarm center. The power alarm also triggered a fire alarm because a break in the continuous electric current always sounded a fire alarm in connection with a power failure alarm.

The alarm center technician in Springfield monitored these alarms. At 3:53 p.m. he saw a signal which indicated that emergency diesels had started and had begun supplying power to the building. The fire alarm at this point was cleared automatically. If a fire had been detected at that time, the fire alarm could not have been cleared. It would have had to be reset manually at Hinsdale.

At 3:59 p.m., additional alarms were received in Springfield which indicated the failure of the emergency diesel power system and the failure of the air dryer equipment. Again, with the momentary interruption of electricity, another fire alarm was activated. One minute later, this alarm was cleared, indicating that there was no detectable fire in the Hinsdale office.

A Springfield technician checked the status of all Hinsdale alarms at 4:05 p.m. This audit indicated the power alarms were continuing, but showed the fire alarm clear.

At 4:16 p.m., the Springfield technician notified the weekend duty supervisor for the Hinsdale area of the power alarms. The supervisor began calling for a technician to visit the Hinsdale building and to make an on-site check of the power system. The duty supervisor was located in Wheaton, a nearby suburb.

At 4:20 p.m., the Hinsdale central office fire alarm again activated. Equipment supervisory alarms followed in rapid succession as the first indications of equipment malfunctions began to appear. At 4:21 p.m., a call being made by the Wheaton duty supervisor to dispatch a technician to check the Hinsdale power alarms was interrupted by a call from the Springfield alarm center. The call from Springfield reported the fire alarm at Hinsdale.

The duty supervisor made a series of calls to dispatch two technicians to Hinsdale and to alert the Hinsdale and Downers Grove fire departments. The calls to the two fire departments failed to go through. Both calls would have had to pass through the Hinsdale central office.

When the first technician arrived at the Hinsdale central office at 4:52 p.m., he found heat and heavy smoke inside the building. He then flagged down a passing motorist and asked him to drive to the fire department about five blocks away. The fire department received the motorist's report at 4:58 p.m. and was at the central office at 5:02 p.m.

Because of the heavy smoke, the source of the fire was difficult to locate. The fire was believed to have been confined to bins of paper records on the first floor of the toll equipment area. While the firemen were attempting to extinguish these burning records, black drops of a melted substance, later identified as molten insulation, dropped down on them bringing the cable tray fire to their attention. Water was sprayed on a small area of fire in the overhead cable racks. At first this appeared to put out the fire.

However, the fire rekindled in the cable rack. Each time water was sprayed on the cables, the fire appeared to go out, but would restart because the cables continued to be energized. Several attempts were made to disconnect power by tripping switches and pulling multiple fuses in the basement of the Hinsdale office. Since a power failure is more likely to interfere with service than a fire, central offices are engineered with multiple backups to protect against power interruptions. All power finally was disconnected about 7:15 p.m. The fire officially was declared extinguished at 11:30 p.m. The Hinsdale fire department and an investigator from the Office of the State Fire Marshal released the building, except for the fire area, to Illinois Bell at 3 a.m., May 9.

B. THE IMPACT OF THE FIRE

The damage caused by the switching station fire affected voice and data communications for more than half a million residents and business customers in Hinsdale and surrounding Chicago-area communities. Local service was disrupted for 38,000 customers in Hinsdale, Clarendon Hills, and Willowbrook and parts of Burr Ridge, Darien, Oak Brook, and Westmont. The outage affected special service lines and local, long distance, and cellular calls because Hinsdale served as a communications gateway for the fiber optic network.

The outage affected businesses and individuals in ways they had never experienced. For example, retailers could not verify credit cards. Many automatic teller machines and the Illinois State Lottery's terminals stopped functioning. The 57-member Suburban Library System was confronted temporarily with piles of books, because returned books could not be recorded in the system since its lines were routed through Hinsdale.

Calls to Information (411), Repair (611), and Illinois Bell customer service centers were affected. The fire interrupted the operation of the JULIE (Joint Utility Locating Information for Excavators) hotline, which provides location information about underground utility facilities for contractors.

While the impacts of the outage were highly individualized and because of sheer volume cannot all be related here, several examples are provided to illustrate the breadth of the potential consequences of such an outage.

A major manufacturer of consumer and industrial products manages its telecommunications services for its Chicago area facilities from an office in Oak Brook, Illinois. The main location in Oak Brook not only houses the telecommunications group, but also a sales office, servicing group, and the administrative department for 13 corporate entities. The Oak Brook Centrex serves this location, plus 9 other Oak Brook locations, 2 Arlington Heights offices, and locations in Bensenville, Hinsdale, and Naperville. In addition to the Centrex service, this company has a nationwide CCSA network provided by AT&T and is served from a System 85 located in downtown Chicago. Access to the network is provided via tie lines between the Centrex in Oak Brook and the System 85 in Chicago. All company locations are in constant contact with the Corporate Headquarters in New York and various other locations nationwide.

The customer's Centrex System was served out of the Hinsdale Central Office. Because 15 company locations are served by the one Centrex System, all 15 locations were completely out of service. The 15 locations, therefore, could not communicate with each other nor with the rest of their locations throughout the country and overseas.

Once it was determined that the Hinsdale 1ESS could not be salvaged, Illinois Bell's Major Business Center, began "rehoming" the Centrex to the Oak Brook 5ESS in order to restore service to the customer as soon as possible. AT&T installed a System 75 at the main Oak Brook location to the AT&T Point of Presence (POP) in Oak Brook to give the customer access to their CCSA network. Once the Centrex was rehomed to Oak Brook, and the tie lines between Oak Brook and the AT&T System 85 in Downtown Chicago were re-engineered, the System 75 in Oak Brook was removed, and normal service was established.

A major general hospital located in Hinsdale has its telephone system separated into two parts: Administration and Patient. Administratively, the telecommunications system is used to conduct the day to day business of the hospital with the outside world. Internally, the communications systems link the various parts of the hospital; e.g., nurses stations, emergency rooms, operating rooms, admissions, and the various labs.

The Hinsdale Central Office fire caused total communications outage to this hospital.

The day following the outage, the hospital was provided with several mobile telephones. The next day several walkie-talkies were provided and 30 FX lines from several central offices were connected for emergency use. In addition, an on-premises PBX System (SL-1) was installed approximately one week from the date of the fire. The new PBX System continues to serve the hospital.

A third example is a manufacturer of farm and construction equipment whose operations are international in scope. This company's Centrex System is used to communicate with its Racine, Wisconsin, headquarters via the company's tie line network, as well as to conduct the day to day normal business functions.

The Hinsdale Central Office fire also caused a total outage of this company's communications system.

Several days following the fire, several FX lines were connected for emergency use. In addition, ten walkie-talkies were provided for their internal use. As an interim measure, the company was sending its critical data via auto and delivery agencies to Racine. Approximately two weeks after the outage a temporary 100 station SL1 on premise PBX system for key telephone users was installed. When the Hinsdale Central Office was restored, the PBX system was removed.

A major retail drug company with approximately 175 stores has its corporate headquarters in Oak Brook, Illinois. Besides being responsible for all telecommunications services, all ordering of inventory (pharmaceuticals, over-the-counter drugs, etc.) is done through the Oak Brook location via data circuits and/or dial up business lines.

The company had three locations that were severely affected by the fire. Two store locations, Westmont and Clarendon Hills, were believed to be completely out of service. Illinois Bell provided one emergency Oak Brook FX line to each location. The Corporate Headquarters in Oak Brook, served by the Oak Brook Central Office, had service, but apparently could only make and receive calls within their serving central office. The drug company activated its disaster recovery plan through Comdisco, which re-established communications with all store locations.

Another major retail drug company which is headquartered in Deerfield, Illinois, was also affected by the outages. The company operates 1,400 retail outlets in 30 states and Puerto Rico. A Northern Telecom PBX services the headquarters' location. There are approximately 50 dedicated private lines that go out to various locations. Long distance is provided by a T1 carrier and the building also houses an 800 system to receive order entries from the stores.

The company uses its communications as a strategic tool. They feel this is the primary strength of their present system. Through their "Intercom Network" a customer is able to have a prescription filled in Illinois and then take a trip to Florida and have it refilled at a company store there. This is a unique application of the communications function in retailing and the company promotes this in their advertising.

The customer's local service was not affected, and although the majority of the Intercom Network is hubbed through the Arlington Heights Central Office, roughly 20 percent of the data circuits for the Intercom Network are hubbed through Hinsdale and were completely out of service.

The company believes that the Hinsdale fire had a severe impact on its ability to provide customer service and compromised the quality of that service.

This company enacted their dial back up system and utilized business lines to transmit necessary data until normal service could be established.

A final example of the effects of the telecommunications disruption is the impact on federal government operations. The Hinsdale Central Office service as a communications apex for air traffic control between O'Hare and Midway airports and the Aurora, Illinois, Air Traffic Control Center (ARTCC). The FAA reported the loss of 28 voice and data circuits between O'Hare and Midway and the ARTCC in Aurora. These circuits constituted ten percent of the circuits between the airports and the Aurora ARTCC. Due to the outage and concurrent storm conditions in the area, approximately 20 percent of the flights out of O'Hare airport were cancelled on Monday, May 9, and extensive backlogs were reported for passengers in other cities. The FAA for safety reasons increased the distance between landing airplanes from 3-5 miles to 20 miles. Despite the disruption in normal operations, FAA did state that the communications loss posed no threat to passenger safety.

The Veterans Administration (VA) initially reported the loss of 23 circuits. These dedicated lines primarily connected VA medical centers and regional offices. Problems with eight additional circuits were later reported. Due to the disruption, VA hospitals and area offices were unable to gain access to the data bases in the VA Chicago Data Processing Center in order to obtain information on veterans being treated or awaiting treatment at VA facilities. Problems with the network were also reported in Philadelphia, Pennsylvania, and Austin, Texas, because of the large amount of information passed between these cities and Chicago.

In addition to the effects of the outage on FAA and VA communications, disruptions in service were reported for several other federal agencies. The federal agencies reporting disruptions in their service were the Department of Commerce, the Nuclear Regulatory Commission, and the Department of Energy.

Businesses solved their communications problems in a variety of ways. One Hinsdale real estate agent rigged her mobile phone so that the car horn would sound when the phone rang, alerting her to run from her office to the car.

Waste Management, Inc.'s headquarters in Oak Brook resumed long distance service by setting up a microwave link from the roof of its building to an AT&T site in Oak Brook. Nalco Chemical in Naperville accomplished the same result by mounting a microwave dish on its building and connecting with a nearby MCI microwave station.

Travel agencies were advised by Illinois Bell to work with their service providers such as American and United Air Lines to expedite restoral of their computer lines. One travel agency, Are You Traveling, temporarily operated in the owner's home and made daily trips to airline offices to collect tickets for its customers.

Hinsdale Transfer Co., a limousine and taxi service, used its vehicles to call on the company's corporate accounts daily for business. The owner also advertised to let his customers know what he was doing and how to reach him. His campaign included a direct mail program in which he mailed "free ride" coupons to residents of ten communities.

The 3M Company's sales office in Hinsdale simply relocated its sales force to an office in Bedford Park, Illinois, and another in California.

Illinois Bell began the restoration of service with the rerouting of interoffice traffic around Hinsdale on available working copper circuits and with the temporary installation of a microwave link between the Hinsdale switching center and the LaGrange switching center. Service for police, fire departments, and hospitals was given first priority for restoral.

Governor James R. Thompson declared DuPage County a disaster area. Federal funding was obtained and the Small Business Administration opened an office in Hinsdale to process applications for loans. The SBA answered 355 requests for loan applications. The Governor's efforts in seeking federal assistance were supported by Congressman Harris Fawell in whose district Hinsdale is located.

The Illinois Department of Commerce and Community Affairs, the Mid-Metro Economic Development Group, and the College of DuPage were joined by Illinois Bell in establishing an Economic Development Resource Center in Hinsdale. One-on-one counseling and a series of economic workshops were offered to help west suburban businesses explore resources available to them.

Special assistance to residential and business customers served from the Hinsdale central office included the following:

- Setting up three special centers with a total of 200 lines in the Hinsdale area to provide interim service to business customers. Calls within the 312 area code were allowed without charge. Bell employees staffed the centers Monday through Saturday from 7 a.m. to 9 p.m. and on Sunday from 9 a.m. to 6 p.m.

- Providing free shuttle bus transportation to one of the centers.

- Installing 120 coin phones at 16 special coin trailer locations throughout the affected area.

- Establishing an Emergency Relay Plan to deliver emergency messages to customers in the affected area. Illinois Bell's Operator Services department provided customers with a toll-free 800 number to call and leave an emergency message. The center would then contact an employee in the field who could deliver the message. The field employee was equipped with a car, pager, and mobile phone. About 150 emergency calls were handled in this manner.

- Interexchange carriers established long distance calling centers.

- Making available 200 lines at 311 W. Washington St. in Chicago for use by business customers.

- Opening a temporary repair center at the Hinsdale switching center to respond to all 611 calls.

- Mailing postcards May 19 to all customers in the affected area with a request that they report lack of service or severe problems by calling 611 or leaving the card with their phone number at one of the emergency coin locations.

C. THE RESTORAL OF THE NETWORK

Restoral proceeded simultaneously on three fronts on an emergency basis. While equipment to provide local service was procured, installed, and tested, other equipment was obtained and installed to allow resumption of network communications to and from the suburbs and to provide access to long distance networks. As this work was underway, Illinois Bell crews were bringing the existing local switching equipment back into temporary service.

The network circuits disrupted by the fire included data links, private line business services, and other special services lines. Also disrupted were interoffice trunks which carry large numbers of calls from one local office to another and to long distance networks.

Customers served by central offices west and southwest of Hinsdale could call one another and reach emergency services within their area, but generally could not make or receive calls from Chicago or long distance points. There were some interoffice circuits that did not pass through Hinsdale, and these provided limited access to the national network.

Even before the fire in Hinsdale was extinguished, network technicians at other locations began rerouting operating interoffice trunk circuits and special services circuits around the affected area using spare capacity on cables that were not routed through Hinsdale. These circuits were used to increase interoffice trunk capacity and provide essential special services.

For example, Illinois Bell re-established the first circuits from the FAA air traffic control center in Aurora to O'Hare Airport before noon the day after the fire. FAA circuits in all priority classes were in place by 4 p.m. May 11.

Microwave dishes were installed on the roofs of Bell's Hinsdale and LaGrange central offices to provide interoffice trunk circuits between these critical points. AT&T and MCI temporarily released available circuits for use in rerouting communications around Hinsdale.

The first interoffice circuits were re-established on fiber optic cables by the end of the first week. Additional circuits were re-established day by day thereafter. Normal interoffice trunk circuit capacity was available by May 22.

Restoral of the 36,774 special service circuits was carried out simultaneously with network restoration, but presented special problems. Restoring these circuits involved locating records containing facility and equipment specifications, re-engineering each circuit, and testing it for the correct operational characteristics.

Rebuilding the fiber optic gateway presented two special challenges: reterminating fiber links between Hinsdale and other end offices and reestablishing severed fiber links before the switching equipment arrived. Fiber restoration practices primarily focus on breaks or cuts of individual fiber links. The break in a single fiber link usually is repaired in a quiet, controlled environment so that significant attention can be given to each fiber. The situation in Hinsdale was almost the opposite. Technicians worked 12-hour shifts and managed to splice 428 individual fibers in 72 hours. Even after the fibers were spliced, the engineers had to verify that the fiber links made the proper connection. To do this, an employee had to be sent to each end office to send back a light beam.

The technicians restored the fiber hub containing toll and transmission equipment for local, special, intra-LATA, and long distance services. The restoral forces rebuilt the fiber hub from the ground up, assembling 63 bays of transmission and multiplex equipment. To expedite the establishment of fiber hub facilities, engineering support personnel moved their computers into trailers on site. Concurrently, more than 55 bays of special service terminal, trunk, and miscellaneous toll and subscriber carrier equipment were installed. In addition, all new cross connect frames were installed to assist in service restoral. Until the fiber hub could get back on line, microwave dishes were set up on the roof to take regional traffic directly out of the Hinsdale switching station.

The switching equipment which provided local service for the Hinsdale area was intact after the fire. However, smoke from the fire combined with the water used to fight the fire formed a destructive acid on metallic surfaces. This acid immediately began to corrode the equipment which survived the fire, rendering it unreliable for providing telephone service over an extended period.

After the fire, Illinois Bell determined that the local equipment, a 1AESS switch, could not be salvaged, and began the process of replacing it. To provide interim service, the existing equipment was cleaned and humidity levels in the building were lowered to retard corrosion as much as possible. This allowed some customers limited use of their telephones within a few days of the fire, a number that grew as more of the equipment was reconditioned.

The number of local customer lines served by the Hinsdale office totaled 41,455. These lines in turn served approximately 38,000 customers. The progress in providing limited dial tone is shown by the table below:

DATE	NUMBER OF LINES WITH DIAL TONE
May 11	12,000
May 13	15,000
May 14	21,000
May 16	27,000
May 17	30,000
May 19	36,000
May 20	Virtually all customer lines now served by dial tone from existing equipment.

While the damaged switching equipment gradually was returned to temporary service, simultaneous efforts were made to install and test a new 5ESS digital switching system. This switch, already enroute from the manufacturer to another telephone company, was diverted to Hinsdale.

During the restoral period, more than 200 people worked in the Hinsdale building 24 hours a day, seven days a week.

Sections of equipment were delivered according to a timetable that brought each piece to the central office as it was needed.

The new switching system was placed in service in two stages. The initial stage was completed May 26 and 19,500 customer lines were transferred to the new switch from the old. The first to be transferred were fire, police and hospital lines.

The remaining customers were transferred June 5. At this point, all service was back to normal. The entire switching system was delivered, installed, tested, and in service four weeks after the fire.

III.

REMEDIAL EFFORTS OF STATE AGENCIES TO DATE

In the days following the May 8 fire, the Fire Marshal's office continued its investigation into its cause. Given the complexity of the incident and the severity of its impact, the Fire Marshal's Office assumed responsibility for the overall investigation from the Hinsdale Fire Department. The Fire Marshal retained the professional services of Professor Emeritus Boyd Hartley of the Illinois Institute of Technology, and of Engineering Systems, Inc. of Chicago to assist it in its efforts.

Staff representatives from the Illinois Commerce Commission (ICC) with technical expertise in telephone engineering made an on-site inspection of the Hinsdale facility on May 10, 1988. They determined that the nature of the fire and the associated effect of acidic residues from the burned electrical insulation would make quick service restoration a difficult task. ICC Staff monitored the around-the-clock restoration efforts to ensure that service was being restored as expeditiously as possible.

On May 13, 1988, ICC Staff initiated its own investigation of the cause and origin of the fire with a view toward developing recommendations for enhancing fire prevention and protection and reducing network vulnerability to any similar occurrence. ICC Staff secured agreement from Illinois Bell to underwrite a professional investigation under the exclusive control of the Staff. ICC Staff interviewed three firms and selected Forensic Technologies International Corporation (FTI), a nationally recognized consulting engineering firm specializing in fire and failure analyses.

Early on, the state agencies recognized that separate investigations would be redundant and, therefore, wasteful and inappropriate. Thus, the investigations were consolidated and FTI was directed to serve as the lead technical investigative party and to carry out its work in a manner consistent with the requirements of the State agencies. The consultants originally retained by the Fire Marshal's Office were then assigned to provide oversight for all of the investigative efforts.

On June 1, 1988, the Illinois Commerce Commission formally retained FTI to perform the following activities:

- Identify the potential sources and causes of the fire and the damage it produced.

- Identify the facts which support each potential cause.

- Determine the most likely cause of the fire and the resultant damage.

- Make recommendations regarding changes in equipment or methods and procedures used to detect, report and suppress central office fires.

- Estimate costs associated with the recommendations.

The Office of State Fire Marshal and the ICC Staff submitted their joint Interim Summary Report in September 1988 (Attachment 4). No conclusions were reached in that report. The final report is due February 28, 1989. We will provide a copy of that report to this Committee.

In addition to this investigation, at the request of Governor Thompson legislation has been introduced in the Illinois General Assembly to establish joint rulemaking authority in these agencies. The adoption of this proposed legislation would enable the agencies to jointly: 1) develop reasonable actions through rulemaking to guarantee that protective mechanisms are established to prevent major interruptions of telecommunications service; 2) develop reasonable actions through rulemaking to guarantee proper emergency response following a telecommunications failure; 3) coordinate and initiate enforcement actions against telecommunications providers that are in violation of the promulgated rules; and 4) aid these agencies in the ongoing regulation of telecommunications, fire protection, and emergency services so as to better protect the interests of the public. A copy of the proposed legislation is attached (See Attachment 3).

Finally, Illinois Emergency Services and Disaster Agency is currently considering the problem of how to design a cost effective system that would enable that agency to communicate with sheriff's departments and fire departments around the state on a system that is not dependent on phone lines. Virtually all of the state's emergency communications systems including its low-band statewide radio net, the National Warning System, the Nuclear Accident Reporting System, and the Federal Emergency Management Agency teletype system are now dependent to a certain degree on phone lines.

One option which IESDA is considering is a statewide, high-band repeater system on which it could gain access to pagers and two-way radios at all locations in the state from the agency's central communications center in Springfield. Systems engineers report that such a system could be designed, but that development could take three to five years to complete and cost several million dollars.

A second option that IESDA is considering is a satellite system that would connect Springfield with every county sheriff's department. Such a system would enable IESDA to send one-way teletype messages to each sheriff's department. Notification to affected fire and police response agencies could then be made county-wide by existing radio and pager systems. If such systems were not in place they could be designed to fit the capabilities and existing needs of the county in question. Figures for satellite systems are not yet complete, but preliminary estimates place the cost much lower than a high-band repeater system.

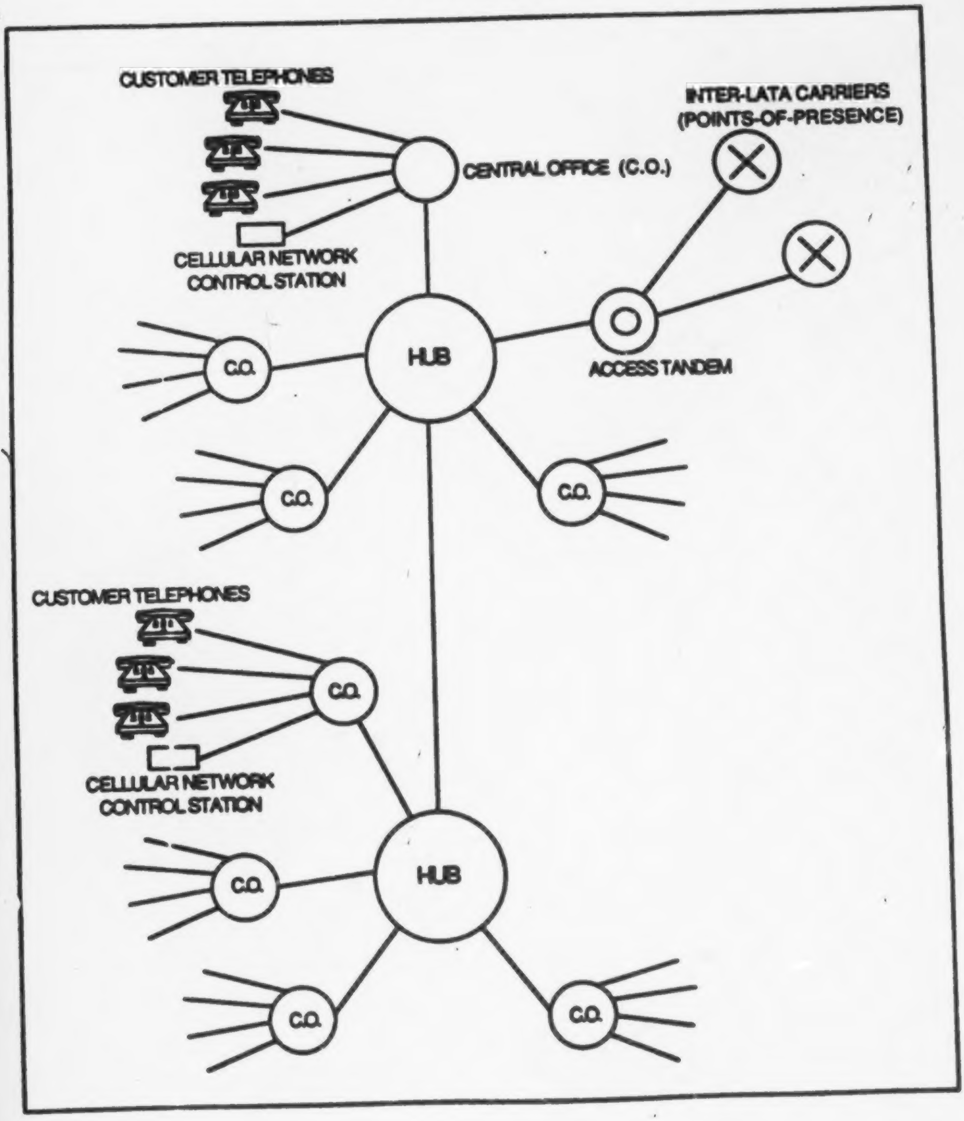
Other options are also being considered. IESDA intends to await the final joint report in order to further define the scope of the problem.

CONCLUSION

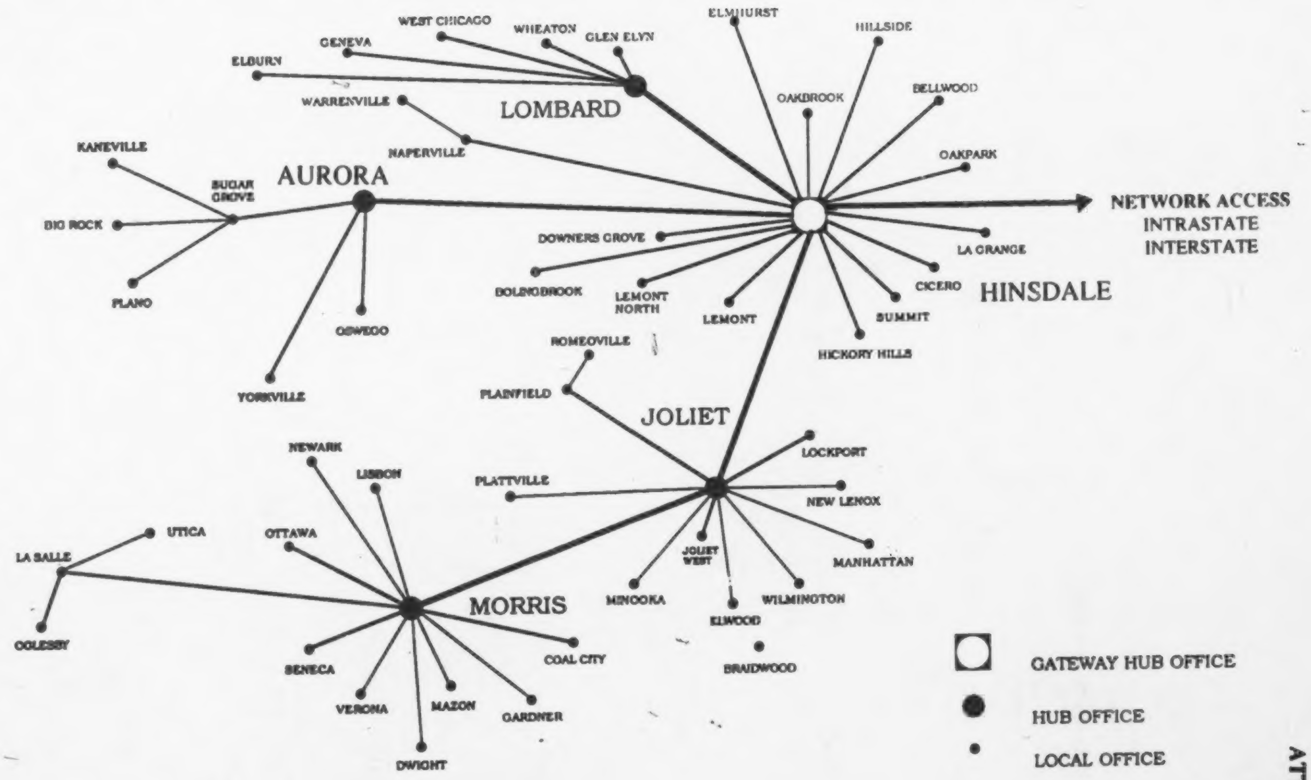
As is evident, the State of Illinois is in a position to make a unique contribution to this Committee's investigation. More information will become available in the near future and will be presented to this Committee. With this information and with the knowledge of steps taken and those which will be taken by the State of Illinois to remedy the impacts of incidents such as the Hinsdale fire, we hope that we have provided this Committee with a useful contribution toward ensuring a reliable national communication network.

ATTACHMENT 1

Hub Configuration


CUSTOMER TELEPHONES
CENTRAL OFFICE (C.O.)
CELLULAR NETWORK CONTROL STATION
INTER-LATA CARRIERS (POINTS-OF-PRESENCE)
HUB
ACCESS TANDEM
C.O.
C.O.
C.O.
CUSTOMER TELEPHONES
C.O.
CELLULAR NETWORK CONTROL STATION
C.O.
HUB
C.O.
C.O.

ATTACHMENT 2


LOMBARD
AURORA
HINSDALE
JOLIET
MORRIS
NETWORK ACCESS
INTRASTATE
INTERSTATE
ELBURN
GENEVA
WEST CHICAGO
WHEATON
GLEN ELYN
ELMHURST
HILLSIDE
OAKBROOK
BELLWOOD
OAKPARK
LA GRANGE
CICERO
SUMMIT
HICKORY HILLS
LEMONT
LEMONT NORTH
BOLINGBROOK
DOWNERS GROVE
WARRENVILLE
NAPERVILLE
KANEVILLE
SUGAR GROVE
BIG ROCK
PLANO
OSWEGO
YORKVILLE
ROMEOVILLE
PLAINFIELD
PLATTVILLE
LOCKPORT
NEW LENOX
MANHATTAN
WILMINGTON
JOLIET WEST
ELWOOD
MINOOKA
BRAIDWOOD
NEWARK
LISBON
OTTAWA
UTICA
LA SALLE
OGLESBY
SENECA
VERONA
DWIGHT
MAZON
GARDNER
COAL CITY
GATEWAY HUB OFFICE
HUB OFFICE
LOCAL OFFICE

HINSDALE CENTRAL OFFICE AND OTHER OFFICES

ATTACHMENT 3

HB 207
Cowlishaw
McCracken

SB 55
Topinka
Zito

86th GENERAL ASSEMBLY

State of Illinois

1989 and 1990

INTRODUCED ______________ , BY

SYNOPSIS: (New Act)

Authorizes the Illinois Commerce Commission, the Office of the State Fire Marshal and the Illinois Emergency Services and Disaster Agency to adopt joint rules on the provisions of adequate fire protection and emergency notification systems at telecommunications service facilities in Illinois. Effective immediately.

LRB8601589RCmbA

A BILL FOR

AN ACT concerning fire protection and emergency services relating to telecommunications facilities.

Be it enacted by the People of the State of Illinois, represented in the General Assembly:

Section 1. The General Assembly finds that telecommunications services have developed into an indispensable facet of modern life, encompassing personal communications, business communications from the local to the international level, and a wide range of emergency communications. The results of any major interruption of telecommunications services can be catastrophic. It is therefore crucial that the State of Illinois take all reasonable actions to provide assurances that appropriate protective mechanisms are in place to prevent major interruptions of telecommunications services and to provide assurances of a proper emergency response if such protective mechanisms fail. The intent of this Act is to authorize the three State agencies most directly responsible for telecommunications, fire prevention, and emergency services, respectively, to develop joint rules and implement enforcement action where necessary to provide such assurances.

Section 2. In addition to any other rulemaking authority they possess, the Illinois Commerce Commission created by "The Public Utilities Act", approved June 29, 1921, as amended, the Office of the State Fire Marshal created by "An Act relating to the State Fire Marshal", approved July 21, 1977, as amended, and the Illinois Emergency Services and Disaster Agency created by the "Illinois Emergency Services and Disaster Agency Act of 1988", approved June 30, 1988 are authorized to adopt joint rules on the provisions of adequate fire protection and emergency notification systems at telecommunications service facilities in Illinois. In adopting such rules, these agencies may consider (a) the need for emergency and other reporting requirements, including without limitation, the immediate notification of the Illinois Emergency Services and Disaster Agency in the event of a major failure of telecommunications systems, and (b) any other matters relevant to the purposes of this Act. Rulemaking proceedings to adopt rules pursuant to this Act shall be conducted under the auspices of the Illinois Commerce Commission in accordance with Article X of the Public Utilities Act and the Illinois Administrative Procedure Act; provided, however, that no joint rules shall be adopted or changed except upon the concurrence of all three agencies.

Section 3. (a) The agencies listed in Section 2 of this Act shall have the authority to investigate alleged violations of the rules adopted under this Act and to serve a notice of violation upon the affected telecommunications carrier or other communications provider. If the affected telecommunications carrier or other communications provider disputes that a violation has occurred, it shall, within 30 days after receipt of the written notice of violation, file a request for hearing on such violation before the Illinois Commerce Commission. The Commission shall conduct a hearing on such matter and enter an order thereon in accordance with the provisions of Article X of the Public Utilities Act, including the provisions for appeal of any such order. In any such hearing before the Commission, one or more of the listed agencies in Section 2 of this Act shall participate and shall present evidence of the alleged violation.

Section 4. (a) Any telecommunications carrier which fails to correct any violation of the rules adopted under this Act after written notice of violation, or, if the violation is disputed, after final determination of violation including appeal if any, in accordance with Section 3, shall be liable for a penalty not to exceed $10,000 for each violation, and an additional penalty not to exceed $1,000 for each day during which such violation continues. Actions for injunction or mandamus to enforce correction of violations and actions to recover penalties authorized under this Section shall be filed in the name of the People of the State of Illinois in the circuit court in accordance with Sections 4-201, 4-202 and 4-203 of the Public Utilities Act. In any action to recover penalties under this Section for a violation determined in any final order of the Commission as provided in Section 3, the fact of the violation shall be deemed proven and shall not be relitigated.

(b) Anything to the contrary in Sections 4-201 and 4-203 notwithstanding, the proceeds of all monetary penalties received from enforcement action initiated pursuant to this Section shall be divided equally between the county and municipality in which the violation occurred.

Section 5. This Act and any rules adopted pursuant to this Act shall be applicable to all telecommunications carriers in Illinois as defined in Section 13-202 of the Public Utilities Act and such other communications providers operating in Illinois as the agencies find are necessary to protect against a major interruption of telecommunications services.

Section 6. This Act takes effect upon its becoming a law.

ATTACHMENT 4

HINSDALE CENTRAL OFFICE FIRE INTERIM SUMMARY REPORT

Joint Report of :
Office of the State Fire Marshal
and
Illinois Commerce Commission Staff

SEAL OF THE STATE OF ILLINOIS
AUG. 26th 1818

HINSDALE CENTRAL OFFICE FIRE
INTERIM SUMMARY REPORT

Joint Report of:

Office of the State Fire Marshal
3150 Executive Park Drive
Springfield, IL 62703-4599

and

Illinois Commerce Commission Staff
527 East Capitol Avenue
Springfield, Illinois 62794-9280

September 6, 1988

Prepared by:

Forensic Technologies International Corporation
2021 Research Drive
Annapolis, Maryland 21401

301/224-8770

TABLE OF CONTENTS

PAGE NO.

1.0 INTRODUCTION 1

2.0 BACKGROUND 1

3.0 INVESTIGATION 2

- 3.1 The Failure Analysis Process 2
- 3.2 Key Issues 2
- 3.3 The Team 3
- 3.4 Investigation Plan of Action 3
- 3.5 Work Completed To Date 7

4.0 OBSERVATIONS TO DATE 8

- 4.1 General Time/Event Scenario 8
- 4.2 Fire Protection 9
- 4.3 Cause and Origin 10

5.0 REMAINING ACTIONS 10

1.0 INTRODUCTION

The fire in the Hinsdale central office of Illinois Bell Telephone Company is now identified as the most serious fire ever encountered by that company. The Office of the State Fire Marshal was on the scene the day of the fire and soon recognized that, due to the nature of the fire and the number of Illinois citizens affected, it should assume, from the Hinsdale Fire Department, the responsibility for the formal fire investigation. The staff of the Illinois Commerce Commission was on the scene two days after the fire and determined that the nature of the fire and the coupled effect of contaminants from the burning of insulation of the wire would make restoration of service most difficult. It was agreed by the Office of the State Fire Marshal and the Illinois Commerce Commission that initial emphasis should be placed on the restoration of service, with the actual evaluation of the cause of the fire to commence after service had been restored.

Realizing the complexity of the investigation to follow, the Office of the State Fire Marshal hired outside professional investigators to assist their efforts in the evaluation. On May 15, Commission staff secured agreement from Illinois Bell to fund the services of an independent professional investigative firm to serve at the exclusive direction of the Commission staff. Commission staff interviewed three investigative firms and selected the firm of Forensic Technologies International, Inc. (FTI). It was recognized early that two different investigations would be inappropriate. A joint investigation would eliminate many redundant operations and would serve to concentrate an in-depth search for the cause, origin, and conclusions. With the merger of the investigative efforts of the Fire Marshal's Office and Commission staff, FTI was directed to serve as the lead technical investigative firm and be responsive to the requirements of both the Fire Marshal's Office and Commission staff. The consultants, originally identified by the Fire Marshal's Office, have been retained by both the Fire Marshal's Office and Commission staff to serve in the overall management of all investigative efforts.

The investigation of an incident of this magnitude must have unquestioned credibility in order to serve the public interest, be of assistance to industry, and serve as a lesson for the improvement of service delivery in the future. To that end, the Office of the State Fire Marshal and Commission staff concurred in having teams of engineers and scientists, representing Illinois Bell and Factory Mutual Insurance Company, participate in the process of the investigation. This approach provided an expanded range of concepts to be considered and tested throughout the evaluation process. Thus far, this concept has served this investigation process well.

The investigation is not complete at this time, and many areas of investigation are still generating findings prior to the development of meaningful conclusions. This report attempts to exclude findings that could lead readers to inaccurate conclusions. The final report will be an unabridged listing of all findings and all conclusions. At this time, the investigation's final report is expected in mid-November.

2.0 BACKGROUND

Late in the afternoon of May 8, 1988, Mother's Day, a fire occurred on the first floor of the Hinsdale Central Office of Illinois Bell, located at 120 South Lincoln Street, Hinsdale, Illinois. As a result of the fire, there was complete loss of phone service to approximately 42,000 local lines and degradation of phone service to another 475,000 lines to outlying areas. Illinois Bell was able to restore partial service within 72 hours and full service within 30 days.

While the fire damage was confined to cable trays near the ceiling on the first floor, extensive damage to telephone communications equipment was caused by the corrosive effects from smoke.

Because the fire was confined to the first floor, and the majority of the second floor was only partially utilized, Illinois Bell was able to completely restore phone service by installing a state-of-the-art replacement central office system on the second floor. This was not only the most efficient method of restoring service, but also provided the opportunity to examine the damaged equipment, in exacting detail, without delaying corrective measures. From June 6, 1988 until present, the investigative team, using FTI in the lead technical roll, has been making exhaustive efforts to thoroughly analyze and evaluate the circumstances surrounding the fire on May 8, 1988.

3.0 INVESTIGATION

3.1 The Failure Analysis Process

In any failure analysis, the methods for discussing the cause of that failure are fundamentally the same. The more complex the failure, the more essential it is to employ and follow the scientific method wherein one can systematically identify, examine, and evaluate all possible causes and/or contributions to a failure.

Before a thorough evaluation of those causes or contributions can be made, every avenue must be explored to understand the exact operational and material condition of the central office on the day of the fire. Under ideal circumstances, a building damaged by fire should remain untouched until thoroughly examined and the cause determined. In the Hinsdale central office, service was restored by installing new equipment in other areas of the building, and the fire damaged area was preserved intact pending the investigation. Evaluations and tests were conducted on and in the damaged area of the building. In order to complete more exhaustive tests, it was necessary to remove the equipment and cables to a company warehouse facility. Care was taken to guard and protect the condition of all equipment and cable thus removed. Essentially, it was necessary to carefully label and document every piece of equipment, every cable, and every piece of evidence that was located in the fire damaged area before moving them to the separate storage facility. In addition, procedures were developed and enacted to address the proper precautions to be addressed in order to follow the legal requirements for chain of custody.

3.2 Key Issues

The key issues being addressed in the investigation are as follows:

1. Fire cause and origin
   This is, by far, the most complex aspect of the investigation. However, the efforts expended in this area are vital to thoroughly addressing all other issues. Every potential cause is being considered and tested against the evidence and facts.

2. Extent of fire damages
   An analysis of the burn and temperature patterns, smoke contaminants, and water effects as a contaminant is being conducted.

3. Fire protection systems
   A thorough review of the existing fire protection system is being conducted to evaluate its adequacy in relation to:

   a. Applicable codes
   b. Common practice
   c. The actual fire that occurred

d. **Future considerations**

4. **Fire detection and reporting systems**
   A thorough review of available data is being conducted to evaluate the:

   a. Powering of alarms
   b. Feasibility of direct alarm to fire departments
   c. Ability to recognize real fires versus false alarms
   d. Building alarm versus central office alarm
   e. Alarm monitoring and interpretations

5. Central Office building structure and equipment
   An evaluation is being made to assess the:

   a. Design of the central office
   b. Equipment functions and operational configurations

6. Fire suppression equipment and techniques
   An examination is being conducted to assess the knowledge and the ability required for fire departments to fight central office fires.

3.3 The Investigative Team

To thoroughly analyze the complex circumstances surrounding the fire at the central office requires many engineering and operational disciplines. The investigative team was directed by the Office of the State Fire Marshal and the Commerce Commission staff, with contractual assistance of professional investigators, to provide overall management. The firm, Forensic Technologies International, Inc. (FTI), was directed to serve in the lead technical role of the investigative process. To that end, they were required to generate the overall plan of investigation and coordinate all subsequent activities. FTI provided the depth of resource needed by assigning six (6) experts from its staff, whose background and areas of expertise cover:

- Fire Cause and Origin
- Electrical Engineering
- Power Utility Engineering
- Fire Protection Systems Design
- Fire Fighting Practices
- Electric Cable and Equipment Fire Characteristics
- Metallurgy

In addition, engineering and scientific assistance was provided by firms including Ameritech, Bellcore, Anderson Engineering Corporation, and Illinois Bell Telephone Company.

3.4 Investigation Plan Of Action

A comprehensive, multi-phased approach was developed at the outset of the investigation and was modified, as necessary, to ensure that the analysis would be properly timed and thoroughly conducted.

Phase I - Site Documentation and Data Collection

Phase I involved gathering of all pertinent data which led to a clearer understanding of the operational and material condition of the central office the day of the fire. Before a confident analysis can be made, it is critical that there is a clear understanding of the sequence of events: 1) activities leading up to the fire, 2) operational configuration at the time of the fire, 3) actual fire suppression techniques employed, and 4) the nature of resultant damage. Because the central office is being restored, extensive, meticulous documentation of the entire burn area was completed prior to removal of equipment to the storage facility. The following is a detailed breakdown of the Phase I approach.

A. Photo Documentation - Every aspect of the fire area from the day of the fire through complete removal, was thoroughly photographed for analysis and historic documentation. This documentation involved both 35mm still photography, as well as videotape. To thoroughly document the site for analysis, the following process was utilized:

1. Photographed all equipment, cables, burn area, burn pattern, etc.
2. Organized photographs into notebooks for review by sequence of photographs.
3. Entering captions of photographs and other pertinent information into computer database.

B. Obtaining and reviewing existing technical drawings.

C. Recreated the burn area configuration by developing simplified, accurate as-built drawings which reflect:

- Basic Burn Pattern
- Air Duct Configuration
- Equipment Location
- Cable Tray Lay-Out
- Cross-Reference Grid
- Fire Detection System

D. Power Cable and Equipment Identification - Because of the complexity of the cable configuration, the exact placement of all power cables within the burn area related to the source and equipment they feed is being developed. To do so, each cable and equipment bay has been tagged and documented prior to removal. To do so in conjunction with removal, the following process was utilized:

1. Tagged and documented equipment bays and power cables feeding into each bay.
2. Removed all bays and located at the storage facility.
3. Removed communication cables from cable trays.
4. Examined, photographically documented, and traced power cables.
5. Removed power cables and located at the storage facility.

E. Evidence Collection and Handling

1. Adapted and employed an efficient evidence handling procedure satisfying the laws concerning chain of custody.
2. Identified specific items of interest, both damaged and undamaged, to be used for testing in the analysis phase.
3. Segregated samples from general evidence.
4. Coordination with other investigators to provide them with test samples.

5. Review and approve all proposed tests.

F. Interviews - Conduct interviews of all individuals who were involved with the central office the day of the fire, had dealings with the central office prior to the fire, or have knowledge pertaining to the material conditions and/or operational configuration of the central office.

G. Miscellaneous Documentation Collection - Gather all pertinent documentation which assists in describing the sequence of events, site configuration, material condition, and surrounding circumstances.

Phase II - Fire Cause and Origin Analysis

Phase II is the actual analysis of the acquired data and physical evidence for the purpose of establishing the cause and origin of the fire. This phase has been occurring whenever practical, concurrently with Phase I. To establish the cause of the fire, it will be required to identify, through physical inspection and analysis, the most likely point of origin. We currently anticipate the point of origin to be within cable tray sections from the center of the burn area, which were carefully cut and stored intact for analysis, which is now underway. Once the point of origin is identified, a coordinated analysis of all data and information will be conducted to explain the most probable cause of the fire. The following is a detailed breakdown of the Phase II approach.

A. Determine the most probable origin of the fire.

   1. Examined the burn areas and evaluated damage.
   2. Identified the most probable areas of origin.
   3. Carefully cut and lowered cable tray sections from the overhead, transferred to storage and documented for analysis by the following:
      a. Tagged, identified by characteristic, and traced, by continuity tests, all power cables.
      b. Conducted an ultraviolet scan to identify material scatter patterns not visible under normal light.
      c. Produced radiographs to identify all anomalies for the most efficient and effective internal analysis.
   4. Carefully dissect cable tray sections based on radiograph results.

B. Construct a computer model of the building, including power system components, cables in their trays, fire detection and suppression systems, and building environmental controls.

C. Once the most probable point of origin is identified, an analysis will be conducted to identify the cause by:

   1. Carefully examining all affected power cables.
   2. Manipulating the computer database to trace the affected cables source to load.
   3. Reviewing the time line to establish sequence of events affecting suspected cables.
   4. Reviewing available documentation and interview notes in light of the affected cables.
   5. Conducting appropriate tests.

6. Utilizing the computer model to replay and analyze various scenarios.

D. Review all facts relative to the failure, postulate basic assumptions, and develop a theory of failure.

E. Examine all circumstances surrounding the theory of cause and formulate possible remedial actions for the prevention of similar fires and resulting damages.

Phase III - Fire Protection Analysis

In addition to understanding why there was a fire, it is very important to examine what fire detection and suppression systems were in place to deal with the fire and evaluate their effectiveness. The final report will present recommendations, as applicable, for improvements which may be made to minimize the risk of and the resultant damage from future fires. To do so, it has been necessary to examine the collected data involving building design, fire detection/suppression systems in place, and fire fighting techniques employed. The following is a detailed breakdown of the Phase III approach.

A. Review Available Data (Site Specific)
  1. Visited the Hinsdale Central Office and observed the general layout, building construction, and design.
  2. Reviewed construction drawings.
  3. Reviewed drawings dealing with fire detection systems.
  4. Obtain and review fire detection operations manual and/or system specifications.
  5. Review fire characteristics of cables by type and quantity to establish fire load.
  6. Review historic and contemporary codes and standards applicable to the central office.
  7. Review the time line to examine the event from first detection through extinguishment.
  8. Review composite interview notes.
  9. Review any pre-fire plans and fire drill procedures.
  10. Employ the computer model in analysis of adequacy of various fire suppression coverage.

B. Compare with applicable codes and/or standard practices
  1. Building design
  2. Fire detection systems
  3. Fire suppression systems
  4. Fire Department response
  5. Building and telephone equipment alarm system

C. Address the following areas within the final report:
  1. Combustibles
  2. Physical structure
  3. Fire protection systems
    a. Detection
    b. Suppression
  4. Fire fighting procedures
  5. Personnel responses
    a. IBT

b. Hinsdale Fire Department and adjoining community fire departments

Phase IV - Final Report

Upon completion of the analysis phases, the written report will present findings and conclusions as to the cause and origin of the fire, the fire protection systems employed and recommendations for remedial actions to be carried out. This report will discuss the following:

1. Material and operational condition of the central office on May 8, 1988.
2. The cause and origin of the fire and the resultant damage.
3. The supporting facts to the theory of cause.
4. Fire protection and suppression.
5. Site monitoring.
6. Personnel training.
7. Recommendations for changes or modifications in equipment or methods and procedures used to: minimize the risk of, detect, report, and suppress central office fires.

3.5 Work Completed To Date

All efforts to date have been directed to: investigating and securing the evidence from the fire scene before pertinent information was lost; gathering background information; conducting interviews with key personnel; and, developing tracking systems on computer databases to efficiently analyze collected data. Thus far, the investigation team has:

1. Taken, processed, and organized approximately 1,750 photographs.

2. Gathered and organized approximately 500 photographs taken by non-FTI personnel.

3. Taken approximately 15 hours of video footage.

4. Interviewed numerous witnesses whose involvement at Hinsdale in some way contributes information to reconstructing the incident.

5. Traced, tagged, and documented all power cables in the area of interest.

6. Identified, tagged, and documented all equipment bays.

7. Set up an evidence management system.

8. Identified and logged all evidence at the storage facility.

9. Conducted various radiograph and x-ray tests on cables and fuses.

10. Conducted ultraviolet scans on suspected fire origin sections.

11. Conducted flammable substance gas chromatograph tests on floor level samples from the area of origin.

12. Collected and tagged numerous samples for testing.

13. Conducted extensive literature searches using national computer data services to compile all available information concerning:

    a. Similar communication facility fires.

    b. Current applicable fire detection and suppression systems.

    c. Fire protection design methods.

    d. Contemporary fire fighting techniques.

    e. Relevant research on electric cable and telephone equipment fires.

14. Reviewed various as-built drawings dealing with building design, cable tray layout, equipment placement, fire detection systems, ventilation systems, and ac and dc power distribution. Verified existing drawings and created accurate, simplified as-built drawings detailing the area of fire.

15. Developed a computer database to describe and locate all power cables related to the burn area that have been cut, tagged, traced, and logged. A significant amount of data entry is complete.

16. Developed a computer database to create an accurate time/event matrix from the many sources of data. Documentation is being screened such as interview notes, 611 trouble call logs, equipment alarm logs, and fire department radio tapes for the purpose of extracting time/event information for data input.

4.0 OBSERVATIONS TO DATE

In failure analysis, it is necessary to thoroughly examine all available evidence and data and to reconstruct, either physically or theoretically, the incident, prior to drawing any conclusions. Because this analysis process is ongoing, it is not possible to present any conclusions in this interim summary. Additionally, it would not be prudent to present any assumed information, which may prove inaccurate at the conclusion of this investigation. Therefore, the following discussion will only contain information that is based on corroborated facts.

4.1 General Time/Event Scenario

The fire occurred in the late afternoon and early evening of Sunday, May 8, 1988. Because it was Mother's Day, the central office was experiencing a high level of telephone call traffic. The office was unmanned and secured, while being electronically monitored from a remote station in Springfield, Illinois.

The first indication of any abnormal conditions at the central office came through a trouble alarm in late afternoon. After the specified procedure for verifying alarms was conducted, the duty supervisor for the Hinsdale Central Office was notified. This supervisor, in turn, notified the emergency response technicians and the Illinois Bell after-hours information center. The duty supervisor then attempted to call the Hinsdale and Downers Grove Fire Departments from Wheaton, with no success. The call was blocked due to damage to the toll trunks coming into the office as a result of the fire. As soon as the first emergency response technician arrived at the central office, he saw heavy black smoke and had a passing motorist notify the fire department while he prepared the building for their entrance. After notification, the Hinsdale Fire Department was on the scene within 5 minutes. Because the fire involved live electrical wiring, it proved difficult to extinguish. The fire was declared under control at about 7:00 p.m. and the alarm was officially struck-out at approximately 11:30 p.m.

4.2 Fire Protection

A. The Central Office Building

The Hinsdale Central Office Building was designed and constructed in the 1950's and began service in the early 1960's. There is currently a basement plus two stories above grade, although the structure was designed for 2 additional stories for a total of 4.

The building is of masonry construction with brick exterior walls and the interior structure is heavy concrete construction. Floor slabs are 8 inch thick reinforced concrete. There are no combustible materials as part of the structure, and the building appears to meet the criteria for Type 1 construction as defined by the National Fire Protection Association (NFPA) #220 - "Standard on Types of Building Construction." Type 1 construction is the most substantial and fire resistive construction generally recognized by building codes.

The building was well compartmentalized vertically. Certain occupancies in the basement level - such as the boiler room, diesel generator room, cable vault - also were isolated in separate fire rated compartments.

The first floor, which is where the fire occurred, is essentially one large undivided area (except for small service areas - restrooms, lobby, shafts, etc.). The floor area of this room is approximately 14,500 square feet. Most of the telephone communications equipment was in this large room, which is referred to as the switch and toll areas. During the fire, the total building structure performed very well.

B. Smoke Detection Systems

The building was equipped with an ionization fire detection system designed to detect products of combustion released during an incipient fire situation. In the early stages of a fire, combustion by-products (both visible and invisible) are released into the area before any appreciable heat is released. The system that was installed, and was operational, was an early warning, product-of-combustion detection system. Additionally, there were detectors installed in the ducts of the air handling system which were designed to detect the presence of smoke, and shut-off that system, so as to prevent smoke from being distributed throughout the building. (In rooms not involved in the fire, there were different types of detectors, such as an infrared flame detector in the diesel generator room, and heat detectors in other rooms.)

The detectors in the fire area were of the "ionization" type and were located on the ceiling at about 20 feet on center. Upon detection of products of combustion, the system was designed to perform the following actions:

a. Sound an alarm in the building.

b. Illuminate a bulb indicating the area of alarm initiation on an annunciator board near the front entrance of the building and on each floor.

c. Transmit a signal to an Illinois Bell facility located in Springfield, Illinois.

d. Shutdown the building air handling fan system.

There is no evidence at the this time that suggests any malfunctions or abnormal operations of the smoke detection system.

C. Fire Fighting

The Hinsdale Fire Department responded and after initial assessment requested assistance from the mutual aid companies of nearby communities, since these fire companies had a pre-plan for a fire of this magnitude. The fire department had performed yearly inspections at the facility and per the pre-fire planning, initially responded with the use of halon fire extinguishers and avoided the use of water. However, they quickly realized that this approach was not effective and brought in hose lines. The fire department's use of water produced an immediate reduction of flame and heat. However, because the building power supply was designed to be very reliable, the source of electric power was continuous and the fire rekindled. Another hinderance factor was that dense smoke reduced visibility such that the fire fighters could not see the fire which persisted in the overhead cables. After the electric power was cut off, the fire department affected final fire extinguishment.

4.3 Cause and Origin

Because the investigation is actively in progess and not all materials have been examined, it is not appropriate to state a final opinion regarding the cause and origin of the fire of May 8, 1988. Information known at this time indicates:

- The primary fire damage was located in metal cable trays in the ceiling above the active telephone communication system equipment.
- The fire spread to materials below the cable tray and along adjacent trays near the ceiling.
- To date, no evidence has been found to indicate that the cause was deliberate.

5.0 REMAINING ACTIONS

All evidence is now located at a separate storage facility. This evidence is being carefully analyzed and inspected to gain an understanding of the sequence of events. Throughout the examination, items are being selected for detailed laboratory testing to eliminate or corroborate assumptions.

Upon completion of analysis and testing, there will be a comprehensive compilation of all historical records and investigation data. This data and information will then be carefully reviewed to formulate assumptions, theories, and opinions. Attempts will be made to further validate theories and assumptions through detailed computer modeling.

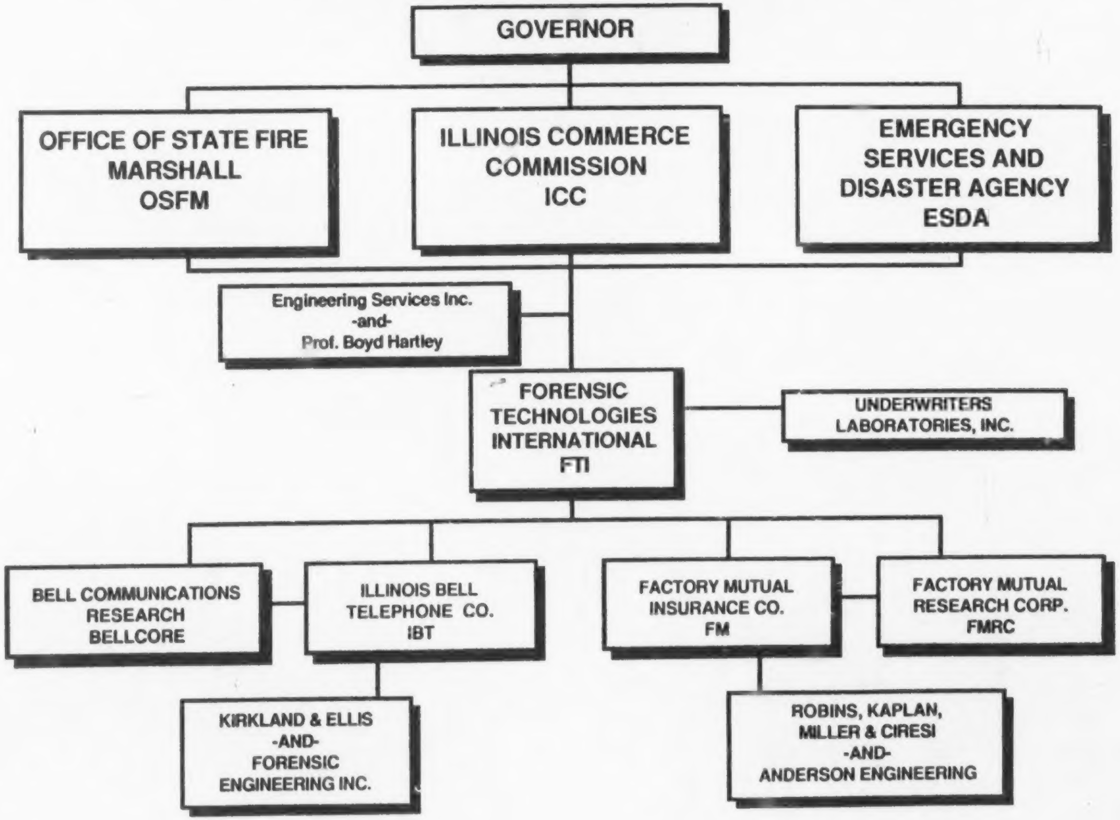
Forensic Technologies International Corporation

2021 Research Drive • Annapolis • Maryland 21401
Annapolis: 301-224-8770 • Baltimore: 841-5545 • Washington: 261-8414 • TELEX (TWX) 710 867-8565

One China Basin Building, Suite 6300 • 185 Berry Street • San Francisco • CA 94107 • 415-398-1995

ATTACHMENT 5

ORGANIZATION IN RESPONSE TO THE IBT HINSDALE CENTRAL OFFICE FIRE


GOVERNOR
OFFICE OF STATE FIRE MARSHALL OSFM
ILLINOIS COMMERCE COMMISSION ICC
EMERGENCY SERVICES AND DISASTER AGENCY ESDA
Engineering Services Inc. -and- Prof. Boyd Hartley
FORENSIC TECHNOLOGIES INTERNATIONAL FTI
UNDERWRITERS LABORATORIES, INC.
BELL COMMUNICATIONS RESEARCH BELLCORE
ILLINOIS BELL TELEPHONE CO. IBT
FACTORY MUTUAL INSURANCE CO. FM
FACTORY MUTUAL RESEARCH CORP. FMRC
KIRKLAND & ELLIS -AND- FORENSIC ENGINEERING INC.
ROBINS, KAPLAN, MILLER & CIRESI -AND- ANDERSON ENGINEERING

ATTACHMENT 5a

Forensic Technologies International Corporation

PROFESSIONAL STAFF BIOGRAPHICAL OUTLINE

JOSEPH R. REYNOLDS, Jr., P.E.

SUMMARY

Electrical Engineer with 18 years large loss fire and failure analysis experience. Internationally recognized expert. Team leader and primary testifier in large multi-disciplinary investigations addressing fire cause and origin, fire and smoke spread, toxicity of fires, fire fighting techniques and fire protection in commercial, industrial and utility applications. Experience and expertise also encompasses power plant major equipment, malfunctions and fires. Electric utilities generating and distribution systems problems. Analysis of nuclear and fossil plant major components, base load generators and main transformers, as well as gas turbine generators and distribution transformers.

ACADEMIC BACKGROUND & REGISTRATION

B.E.S. Electrical Engineering, The Johns Hopkins University, 1969
A.A.S. Electrical Technology, The Capitol Institute of Technology, 1964
Postgraduate Studies, Engineering and Mathematics, The Johns Hopkins University 1970 - 1972
P.E. Electrical Engineering, Maryland, 1973

EXPERIENCE

FTI, Annapolis, Maryland, 1975 - present, President

Team leader and principal investigator on numerous major fire loss investigations, including:

- **MGM Grand Hotel Fire, Las Vegas, Nevada, 1980 to 1985**

  Acted as team leader for multi-discipline investigation of fire and smoke spread related to high rise structures, fire protection, toxicology, electrical systems, codes and regulations regarding paths of fire and smoke spread related to deaths and injuries in those paths. Also developed 2 hour time line incorporating thousands of data points. Provided expert testimony.

- **New World Tower Electrical Fire Investigation, Miami, Florida 1986 to 1988**

  Investigated cause of electrical failure/fire in network transformer vault under high rise office building. During the failure, PCB-laden oil and other insulation ignited, leading to concern about contamination of the building. Directed toxicological analysis team to assess diminished value claim. Provided expert testimony.

- **Turkey Point III, Generator Failure, Florida Power & Light, 1981 to 1982**

  Addressed 700 megawatt generator core burn, including cause of failure, extent of damage and recommended loss prevention techniques for similar installations. Analyzed design criteria for large generator applications. This investigation led to further investigations of similar failures in Brazil and at the Martin Plant in Florida.

- **Nuclear Reactor Thermal Shield**, Florida Power & Light, 1984

  Functioned as team leader to address a seriously cracked thermal shield to a nuclear reactor. The investigation included the development of a loss-prevention program, the production of a report submitted to the Nuclear Regulatory Commission as a major portion of the Risk Assessment Analysis required to maintain the plant's license to operate; a complete technical presentation, and operating models for use in Public Service Commission hearing. Team members served as objective, independent technical spokespeople for the utility.

- **Underground Cable Failure**, Malaysia, 1985 - 1987

  Acted as project engineer on telecommunications/power cable failure investigation concerning 120 miles of cable installed across the country. Developed test procedures for determining the extent of damaged cable installed. Provided procedures for improved installation techniques and replacement of damaged cable. Initiated a new schedule of completion which was satisfactorily completed.

- **Ocean going Vessels**, various

  Investigated cause of engine room fires and evaluated ship construction, fire detection and suppression systems and fire-fighting techniques on ships and tugs.

- **Other Analyses:**

  - Gasoline pump failures and fires
  - Food processing plant fires
  - Paint spray fires in industrial plants
  - Propane and natural gas fires and explosions
  - Power plant boiler fires
  - Manufacturing plant fires
  - Grain elevator explosions
  - Electrical transformer and equipment fires

Trident Engineering, Annapolis, Maryland, 1969 - 1975

Director and principal research engineer initiated forensic engineering department and directed and conducted over 100 failure investigations primarily in the areas of fires, explosions and electrical failures. During early forensic engineering work, developed an excellent reputation among insurance companies on large loss failures and fires across the United States and internationally.

The Johns Hopkins University, Baltimore, Maryland, 1966 - 1969

Research assistant assigned to the effects studies group utilizing a 50 Mev Van deGraff generator laboratory. Responsibilities included designing all electronic systems for use in this research under the direction of the Physics Department. Also assigned to Carlyle Barton Laboratory where work involved classified electronic warfare projects concerning airborne and anti-aircraft radar systems.

Department of Defense, Fort George Meade, Maryland, 1965 - 1966

Engineering Technician assigned to the N.S.A., performed classified work.

SOCIETIES AND MEMBERSHIPS

American Society of Safety Engineers
Dielectrics and Electrical Insulation Society
Institute of Electrical and Electronics Engineers, Inc.
International Association of Arson Investigators
National Fire Protection Association
National Society of Professional Engineers
Power Engineering Society

RESEARCH ACTIVITIES

Electronic Systems, High-Energy Physics, Fire Science, Electrical Insulation

PUBLICATIONS

"Generic Guidelines for the Life Extension of Plant Electrical Equipment", Electric Power Research Institute, July 1988.

"Least Cost Gauge Buoy for Measurement and Analysis of Ocean Waves", International Symposium on Ocean Wave Measurement and Analysis, September 1974, Vol. 1, p. 639, A.S.C.E.

12/88vml

FORENSIC TECHNOLOGIES INTERNATIONAL CORPORATION (FTI)

FTI is an engineering consulting firm that specializes in the research and analysis of unusual and controversial technical problems. Professional services offered range from quick reaction on-site investigations to long-term, multifaceted technical studies. All tasks are managed and directed by an experienced staff to provide practical answers and guidelines for direct application by the client.

Since Forensic Technologies International was formed in 1969, its staff of over 150 consulting engineers, scientists, and experts in specialized fields, has developed an international reputation for expertise and thoroughness in the field of failure analysis, risk assessment and loss prevention. FTI's ability to develop a creative approach to problem solving has been honed while providing expert services for nearly 6,000 failure and risk analysis situations. Each one of these cases possessed unique characteristics that had to be addressed with scientific objectivity, thoroughness, and attention to detail appropriate to development of evidence and expert testimony for public service commissions, regulatory agencies and before the court. Clients have included electric, gas and communications utilities, public service commissions, and other segments of the utilities industry, and both the legal and insurance communities. FTI's basic method for provision of services is to organize and control a team of experts, whose unique backgrounds and capabilities assure achievement of the highest possible degree of certainty for a requested analysis.

Failure analysis and related consulting services typically involve the following activities:

- data collection (evidence, reports, statements, data base),
- Data transfer (interviews, meetings, consultations, mainframe to microcomputer),
- analysis (application of expert services, data manipulation),
- presentation (written and oral reports to professional counterparts, commissions, boards or in court).

The FTI failure analysis process, furthermore, encourages a creative approach to problem solving, because each project must be investigated and analyzed on its own merits, without resort to a fixed or traditional method that might be sufficient for non-forensic companies. Failure analysis logic demands that all possible causes and contributing factors to a failure or loss be identified, then systematically analyzed and weighted to develop a "most probable" cause. This fundamemtal approach corresponds to the identification, classification, and evaluation of risks in the proposed risk assessment project.

During the past decade, FTI has been involved in investigating major fire losses all over the world. The following is a list of the most widely known:

- The MGM Grand Hotel Fire - Las Vegas, Nevada
- One Market Plaza - San Francisco, California
- New World Tower - Miami, Florida
- Dupont Plaza Hotel Fire - San Juan, Puerto Rico
- First Interstate Bank Fire - Los Angeles, California
- Sinking of Superservent II - Africa
- 700MW Generator Arc and Fire - Brazil

Efforts in each of these cases was extensive, requiring a multi-disciplinary and integrated technical approach. The talents of the FTI staff were combined with the project management experience gained from 15 years of working on large losses, providing clients with the highest quality technical service. In-depth analyses of large fires, and explosions have included:

- Cause and Origin of Explosions
- Cause and Origin of Fires
- Flammability and Flame Spread
- Electrical System Design
- Sprinkler System Design & Operations
- HVAC System Design
- Smoke Migration Analysis
- Toxic By-product Analysis
- Autopsy Blood Data Correlation with Toxic Spread
- Computer Modeling of Toxic Migrations
- Toxicological Analysis
- Computer Animation
- Visual Communications
- Film and Video Production

ATTACHMENT 5b

BOYD A. HARTLEY, P.E.

Emeritus Associate Professor and Chairman
Fire Protection and Safety Engineering Department
Illinois Institute of Technology
Chicago, Illinois

Appointed Assistant Chairman, Fire Protection and Safety Engineering Department, March, 1975.

Appointed Chairman, Fire Protection and Safety Engineering Department, September, 1975.

Appointed Professor Emeritus as of May, 1985.

Current Activities

A. Registered Professional Engineer in the States of New York and Illinois

B. Professional Society Memberships

NATIONAL FIRE PROTECTION ASSOCIATION; MEMBER
Currently member of Committees on:
(a) Public Fire Service Organization and Operation
(b) Accreditation of Fire Protection Education Programs

SOCIETY OF FIRE PROTECTION ENGINEERS; MEMBER
(a) Member and Past President, Chicago Chapter

AMERICAN SOCIETY OF SAFETY ENGINEERS; PROFESSIONAL MEMBER

ILLINOIS SAFETY COUNCIL; MEMBER, EXECUTIVE COMMITTEE OF BOARD OF DIRECTORS AND PAST CHAIRMAN OF THE BOARD

GREATER CHICAGO SAFETY COUNCIL; PAST PRESIDENT

UNDERWRITERS LABORATORIES, INC.; CORPORATE MEMBER
(a) Member, Fire Council
(b) Member, Electrical Council

ASSOCIATION OF RETIRED INSURANCE MEN

HONORARY SOCIETIES AND AWARDS
(a) Tau Beta Pi (Engineering)
(b) Compass and Chain (Civil Engineering)
(c) Salamander (Fire Protection Engineering)
(d) Finnegan Award (1983)

CHICAGO ASSOCIATION OF COMMERCE AND INDUSTRY COMMITTEE ON FIRE PREVENTION

C. Illinois Institute of Technology Activities
(a) Chairman, Fire Protection & Safety Engineering Dept.
(b) Professor Emeritus

D. Consulting Engineering services to municipalities, governmental bodies, and industries, as well as to lawyers as an expert witness in lawsuits involving safety, fires, explosions, fire alarms, and fire department organization and administration.

Publications

1956 - "The Grading Schedule of the National Board of Fire Underwriters and What It Means to a City"; published in Municipal Signal Engineer, Nov. - Dec.

1957 - "Standards for Municipal Fire Alarm Systems"; published in Municipal Signal Engineer, Nov. - Dec.

1959 - "Discussion of Revisions to the Standard for Municipal Fire Alarm Systems, NBFU No. 73"; published in Municipal Signal Engineer, Jan. - Feb.

1960 - "Private Fire Alarm Systems and the Municipal Fire Alarm Superintendent"; published in Municipal Signal Engineer, May - June.

1962 - Handbook of Fire Protection, 12th Edition, published by the NFPA. Responsible for revising the Chapter on Municipal Fire Alarm Systems and assisting in revision of the Chapter on Private Alarm Systems.

1967 - "Fire Protection Engineering: Who Approves What?" published in Actual Specifying Engineer, June, 1967.

1967 - "Elements of Fire Department Management and Operation: A Statistical Analysis"; published in the Yearbook of the International City Management Association. This article is based on the information gathered by preparing a questionnaire, distributing it to approximately 3,000 cities of over 5,000 population, tabulating the data returned and interpreting the answers and trends through the author's experience. Salaries and aspects of working conditions are discussed.

1967 - "Fire Alarm Communications"; published by the International City Managers' Association as a component of their Management Information Service. A discussion of various design features and problems of installation and operation including false alarms.

1968 - "A Statistical Analysis of Fire Department Salaries"; published in the Yearbook of the International City Management Association. Information gathered as above in Item 7; salaries are compared with other workers, both public employees and industry.

1969 - "Fire Department Personnel Practices"; published in the Yearbook of the International City Management Association. Information gathered as above in Item 7; salaries are compared with other workers, both public employees and industry.

1969 - Handbook of Fire Protection, 13th Edition; published by the NFPA. Responsible for revisions to the chapter on Municipal Alarm Systems.

1970 - "Fire Department Unionization"; published in the Yearbook of the International City Management Association. Information gathered in Item 7, above. Trends in union contracts and extent of union growth.

1970 - "Emergency Medical Services"; published in the Yearbook of the International City Management Association. Information developed as in Item 7, above. Where do citizens get this service, how is it controlled or regulated if privately operated, what special problems are there?

1971 - "Fire Department Training"; published in the Yearbook of the International City Management Association. Information developed as in Item 7, above. What training should be given and what is given, is junior college education required, and what training facilities are available?

1975 - "Design Approval Authorities and Agencies"; Chapter 3 of the book, Fire Protection for the Design Professional, edited by Rolf Jensen, P.E., published by Cahners Books.

1977 - "Smoke Detectors"; a newspaper article published in whole or in part by 35 newspapers in the Chicago Metropolitan area.

ATTACHMENT 5c

ESI
Engineering Systems, Inc.
550 N. Commons Drive, #102, Aurora, Illinois 60504
(312) 851-4566

EDWARD W. HOLMES
PRINCIPAL ENGINEER

Mr. Holmes is Principal Engineer and Co-Founder of Engineering Systems, Inc. During the past 25 years he has demonstrated expertise in engineering management, process development, quality control, product development, failure analysis, accident reconstruction, materials research and consulting engineering. Mr. Holmes specializes in material failure analysis, industrial safety, aviation, consumer products and fire cause and origin.

Engineering Systems, Inc. was founded in 1987 as an independent engineering consulting firm and laboratory providing professional technical services to industrial and insurance companies, and legal and other professional firms. Mr. Holmes is a project manager and engineer on a variety of engineering investigations.

Professional Affiliations:

American Society for Metals International (ASM)
  National Membership Committee
  Past Chairman of Chicago-Western Chapter
  Chairman
  Treasurer
  Secretary

The Metallurgical Society of the AIME (TMS-AIME)

International Society of Air Safety Investigators (ISASI)

Certified Products Safety Manager (CPSM)

National Fire Protection Association (NFPA)

Illinois Advisory Committee on Arson Prevention

Education:

Master of Science, Metallurgical Engineering
University of Wisconsin - 1965
Bachelor of Science, Metallurgical Engineering
University of Wisconsin - 1962
Additional graduate work at the University of Illinois
Chicago

Positions Held:

Engineering Systems, Inc.
Principal Engineer, Co-Founder, Treasurer, 1987

Packer Engineering Associates, Inc.
Director, Metallurgical Engineering, 1984-1987
Director, Safety Engineering, 1978-1984

Continental Can Company
Manager Techno-Economic, 1978
Manager Metals Development & Surface Phenomena, 1975-1978
Project Manager, 1973-1975
Senior Metallurgist, 1968-1973

Exxon Research & Engineering
Metallurgical Engineer, 1965-1968

Beloit Corporation
Foundry Quality Control Metallurgist, 1962-1964

Publications and Technical Presentations:

C. R. Morin, E. W. Holmes, M. J. Grycko, S. L. Meiley, D. F. Bowers, K. F. Packer and Z. B. Flanders, "Analysis of Causative Factors of the MEA Absorber Vessel Rupture, Chicago, Illinois, July 23, 1984", PVP Vol. 109.

E. W. Holmes "Tutorial - Failure Analysis", Mayfield Grossmann Seminar, ASM, Chicago-Western Chapter, May 13, 1987.

E. W. Holmes, "Analysis of Causative Factors of the MEA Absorber Vessel Rupture, Chicago, Illinois, July 23, 1984". Symposium on ASME Codes and Recent Advances in PVP and Valve Technology, Chicago, July, 1986.

E. W. Holmes, "Failure Analysis - Case Histories", ASM, Valparaiso, February 19, 1987.

E. W. Holmes, "Product Liability", ASM, Rockford, summer of 1985.

E. W. Holmes, "A Users Look at Continuously Cast Steel", ASM, Chicago-Western Chapter, October, 1977.

Other Rating:

Mr. Holmes is an Instrument-Rated Private Pilot.

1-89

Statement
of
John C. McDonald
Chairman
Committee on Review of Switching, Synchronization and
Network Control in National Security Telecommunications
National Research Council
National Academy of Sciences--National Academy of Engineering
Before the
Committee on Governmental Affairs
United States Senate

February 7, 1989

A. Introduction

Mr. Chairman and Members of the Committee:

Thank you very much for this opportunity to testify on this most critical topic: the vulnerability of our nation's telecommunications networks. The Committee's interest in this subject is both timely and appropriate, and I do want to commend the Committee and you, Mr. Chairman, for your interest.

I should note that I appear here today as the Chairman of the Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications. While I am also Executive Vice-President, Technology and a member of the Board of Directors of Contel Corporation, I do not appear here as a representative of Contel, and the views I express may not necessarily be shared by my company.

My Committee was established in November, 1986 by the National Research Council, the principal operating agency of the National Academy of Sciences and the National Academy of Engineering, at the request of the Manager, National Communications System ("NCS"). My Committee was charged with examining the capability of the public switched networks to provide service for purposes of national security emergency preparedness ("NSEP"). I wish at the outset to commend the NCS for its diligence in carrying out its mission. I also wish to commend the National Security Telecommunications Advisory Committee ("NSTAC") for bringing together industry and government representatives to address NSEP issues.

The Committee is composed of fourteen members, distinguished experts in various aspects of telecommunications, drawn from universities, non-profit organizations, local exchange carriers, inter-exchange carriers, manufacturers, users and independent researchers. By marshalling a broad cross-section of telecommunications expertise, the Committee brought a balance of viewpoints and breadth of experience to its deliberations. During the two years of our work we have sought to build upon the solid work done by the NCS, the NSTAC and two predecessor committees at the Academy.

The Committee first provided the NCS with a quick-reaction report on the suitability of the proposed Nationwide Emergency

Telecommunications Service ("NETS") to support NSEP. NETS is designed to provide voice and low speed data transmission services for 30,000 priority users, as directed by the Manager, NCS. Our quick-reaction report was released in August, 1987.

The Committee's first report concluded that unless changes are made, the public switched networks are and will remain insufficient to support NSEP in the periods before, during and after wartime attack. The report recommended improvements to the public switched networks, of which the following are key: (1) provide more survivable network signaling capabilities; and (2) provide for adaptive routing through damaged facilities. The Committee concluded that NETS is needed now, and will be for the foreseeable future, to provide government users with the priority communications necessary for NSEP purposes. Adequate communications links are essential for vital national security functions, including facilitating the timely termination of war.

In its second phase, the Committee took a broader look at how the public switched networks are expected to evolve out to the year 2000. This enabled us to identify potential network vulnerabilities in general, and the implications for NSEP in particular. The Committee's report will be released this Spring. In this second report, entitled "The Growing Vulnerability of the Public Networks: Implications for Emergency Preparedness," we conclude that the public networks are becoming more vulnerable to major service disruptions. My statement today will focus on these broader network NSEP vulnerabilities.

In order to place the Committee's conclusions and recommendations in proper perspective I want to define for you the type of service interruption we consider major. First and foremost, we are concerned with damage resulting from events that cause massive loss of life. National level programs such as NETS are designed to serve government needs in such emergencies. But our Committee also became concerned about the economic and social dislocations which can result from public switched network failures. Our society is growing ever more dependent upon communications facilities to support the daily operations of government and industry. The consequences of major network service losses will become more serious as societal reliance upon communications becomes greater.

In this context, my basic message today is quite direct. First: Our public switched networks are becoming more vulnerable to disruption because of the introduction of new technologies. Second, because of economic incentives to cut the costs of normal commercial operation today's networks are being designed without sufficient attention to emergency preparedness. Third: Accidents, disasters and attack threaten tomorrow's networks with more extensive damage than they did yesterday's integrated network. Fourth: Our Information Society relies absolutely on smoothly functioning communications networks and thus the consequences of network failure are more severe. And fifth: We can reduce these growing vulnerabilities by strengthening existing governmental resources, improving contingency planning and deploying more robust network architectures.

In the wake of the AT&T Divestiture, the once-integrated nationwide public switched network has become a "network of networks." These networks are operating under increasingly diverging standards, and there has been a proliferation of network architectures that are not fully inter-linked as was the case in the pre-divestiture integrated nationwide network. Network traffic is increasingly concentrated in high capacity trunk lines and is being concentrated at critical central switching nodes; network services increasingly rely on concentrated databases. The organizational segment since divestiture has made crisis management harder for the Manager of NCS, and trends in network topology make the networks less reliable providers of vital emergency services.

Our Committee has had the opportunity to study in depth the current state and future development of America's public communications networks. It is the Committee's firm conclusion that the networks are becoming more vulnerable to disruption, whether caused by natural disasters, industrial accidents, deliberate acts of sabotage or war.

In the past year there have been at least five major service interruptions in the public switched communications networks. In May of 1988 alone, there were two serious disruptions. A switching center outage in Charlotte, North Carolina impaired service to 130,000 customers. Fortunately, that particular interruption in service occurred in the middle of the night, and not during the business day. At Hinsdale, Illinois a major wire center was destroyed by fire. Service in parts of the Chicago area was not fully restored for over a month. Residences were without 911 service; businesses which depended upon telecommunications to contact customers lost millions of dollars in revenues.

In June, an accident at Framingham, Massachusetts disabled a switching center for a whole day. And in November, a graduate student at Cornell inserted a "computer worm" in the ARPANET data network, demonstrating the software vulnerability of communications service networks. While the Cornell worm did not invade the executable code of network switching software, it did penetrate user databases; had the worm been designed to destroy data it could have done so. Also in November, an accidental cut of a fiber optic cable in New Jersey seriously disrupted telephone service for the entire East Coast throughout the day.

Now of course these events are not the first times that the public networks have suffered major outages--a New York Telephone central office in Manhattan burned in 1975. That disaster was the worst ever for the Bell System: full service was not restored for 22 days, although emergency service was on line in 24 hours. Two disturbing changes since 1975 make central office fires more worrisome today: First, changes in the architectural design of the public switched networks are concentrating network assets in mega-switches, that is, switches which can handle perhaps a million calls per hour; and second, there is increased user reliance on telecommunications networks due to computer communications, electronic mail, facsimile and the like. As a result, the consequences of specific outages are likely to be more severe.

Let me now move from the general problem to focus on specific threats to our networks.

B. Threats

Acts of God are major sources of danger to network assets: tornadoes, hurricanes, floods, earthquakes and the like. The Shuttle launch last fall was almost disrupted by Hurricane Gilbert's 175 mph winds, which could have knocked down satellite tracking dishes and associated public network lines had it passed across the Johnson Space Center. Industrial accidents such as an accidental cut of an underground cable or a fire at a central office building can interrupt service. A major industrial accident, such as Three Mile Island, can impair telephone service by creating massive traffic demand which overloads the capacity of the public networks. The result is that when you need the service most, the service isn't there.

Another source of harm is that caused by deliberate human action. As recent events show, outside hackers can illegally enter computer networks via telephone lines. Intruders can follow the example of "Captain Midnight" and capture a satellite receiver with an electronic signal, disrupting television transmission--indeed, it is as easy to disrupt a satellite voice transponder as a television transponder. Disgruntled employees with detailed knowledge of network operating software can invade network operating systems, or outsiders might steal technical manuals and learn enough to penetrate the network from outside.

An especially worrisome threat is that posed by correlated attacks by terrorists. For example, our long distance networks rely upon network control provided by a very limited number of Signal Transfer Points. A few well-placed hand grenades would crash major portions of the domestic long distance networks. For international traffic, there are only a few undersea cables--whose locations are well-known--connecting the United States to

Europe and Japan, although here there is some redundancy available from international satellite service.

Let me turn to the changes in network technology which are making the public networks less reliable providers of emergency services.

C. Technology Trends

Three technologies are heavily influencing the future architectures of networks: fiber optic cables, digital switching and software. While each of these technologies brings substantial benefits to network users, each also creates or amplifies network vulnerabilities.

Fiber optics are revolutionizing the transmission of information. A single fiber has an estimated bandwidth of 20 Teraherz--20 trillion cycles per second--which is sufficient to carry all the busy hour traffic in the United States on the busiest day of the year. The economics of the increasingly competitive telecommunications markets are driving network designers to concentrate more and more communications channels into a single fiber. Although at present fiber deployment has not thinned network trunk routes, economic pressures could stimulate consolidation of trunks, and thus reduce the physical redundancy which has historically characterized the public networks. When the New Jersey fiber cable was cut last November by a construction crew, network capacity of 200,000 calls an hour was lost---millions of calls were lost that day.

Fiber routes selected by competing carriers tend to be physically co-located. Geographic barriers, such as mountain ranges and rivers, impose natural constraints on the selection of routes for communications lines. For example, a single bridge will frequently carry fiber cables from all communications suppliers. Also, fiber rights-of-way tend to follow railway and highway routes.

Increasingly, fiber is becoming the transmission medium of choice. By 1995 the long distance network will be almost exclusively fiber, and fiber is now economical for the lines linking access tandem gateways with local central offices. As fiber supplants copper cable, microwave radio and satellites, network transmission is being deprived of media diversity, a valuable means to back-up communications. Satellites linked to Very Small Aperture Terminals and other forms of radio access must not merely be viewed as market competitors for fiber; their value to the nation as redundant media must be considered by those charged with NSEP telecommunications responsibilities.

A second trend in technology which is amplifying network vulnerabilities is the widespread deployment of digital switching in the public networks. Digital switching systems are compact and can economically serve two to five times as many customers as their analog counterparts. In the past, the sheer size and cost of electromechanical systems limited the number of calls which could be routed by a single system, but digital technology now permits central office switches to handle as many as perhaps a million calls per hour.

While there are approximately 19,000 central switching offices in the United States, this number will decline as the economics of switching drive network topologies toward mega-size central switching nodes. These "host" switches not only directly route enormous volumes of traffic but also provide host support for "remote" switching nodes. Remote switches which depend upon hosts have replaced small stand-alone central office switches. A host-remote architecture of network switching nodes is akin to a mainframe computer which provides support for remote desktop "slaved" workstations: if the mainframe fails, the workstations will also fail.

The final worrisome trend is the greatly increased reliance of the network upon software to control network operations. Some of the intelligence traditionally supplied by the local switching office has been removed and now resides at a small number of remote points accessed by the signaling network. Large switches have software programs of up to 10 million lines of code, and massive databases used for network control create concentration of network software assets. Further, the FCC has mandated that the Regional Bell Operating Companies provide Open Network Architecture ("ONA") to enable non-network based providers to compete with the Bell Companies on an equal footing in competitive telecommunications markets; our Committee was briefed by the FCC on this matter.

While the FCC's purpose in opening the public network architecture is laudable, the practical consequence of opening network software to outside access is a reduction in network database security. While ONA requirements so far have not meant outside access to executable network code, the increase in outside access to network databases is in itself cause for concern. Here again it is a mistake to view network assets solely in terms of their economic role and value; our public networks also have security and emergency capabilities which are critical to our national welfare and, indeed, to our very survival.

ONA will, to be sure, confer real benefits: providers and users can control their networks by reprogramming network software. Network structures can be dynamically reconfigured, reducing communication costs and providing a valuable tool for businesses with high data transmission requirements.

But as with fiber and digital switches there is a downside:

viruses, Trojan Horses, worms and the like. Just how serious the downside can be is illustrated by a recent California case reported in the New York Times. A federal district court judge ordered a computer hacker held without bail, calling him "a very, very great danger to the community." The hacker had illegally entered computers at universities and even at the National Security Agency. He had stolen millions of dollars worth of software from databases, and in 1987, he had compromised the entire telephone switching network of Pacific Bell, according to an internal memorandum obtained by the press. Also, he had acquired the complete "source code" of Digital Equipment Corporation's VMS operating system program, as well as a special related security program. The defendant was denied unsupervised access to telephones during his confinement.

Sophisticated software is also a source of vulnerability in modern network signaling. The purposes of signaling are to route a call through the network and to report on its status--busy, ringing, connected or terminated. Network signaling today is moving towards what is called "Common Channel Signaling." Older technology employed multi-frequency signaling, such as the tone you hear in touch tone telephones when dialing. In the old system, signaling was "in-band"--the network signals were carried in the same channel as the communication; the new system is "out-of-band"--signals are software-created and then carried in a common signaling channel, physically separate from the communication channels. This consolidation of the signaling function creates additional vulnerability.

In a typical call with in-band signaling, the calling party signaled to his originating central office by dialing a number. This number was then sent to the next office over a voice channel which would later be used for the actual conversation. Signaling then proceeded from office to office until the final destination was reached. If the called party's line was busy, a busy signal would be returned over the circuit path of the call to the originating party. Thus, signaling was distributed throughout all the trunks in the network.

Common channel signaling will change that: all signaling takes place over separate data links which connect the switching systems of the network. In a typical application, the calling party signals his central office by using multi-frequency touch tone. The central office, employing common channel signaling, receives the dialed number and the central processor creates a message which is sent over a separate packet-switched network to the destination central office. If the called party is busy, a busy message is returned over the packet network to the originating central office.

This new signaling technology provides much flexibility in processing and routing calls. However, the concentration of the signaling software and hardware into a sub-network means greater vulnerability than if the signaling function were spread throughout entire networks. Without signaling, networks cannot function, so this added vulnerability is a serious matter. As I indicated earlier, the long distance signaling networks depend upon a very limited number of critical packet-switching nodes. While these systems can function under failures at single points, they cannot do so under multiple failures.

Another source of software vulnerability arises from a concept called the "Intelligent Network." These networks employ the packet signaling networks to provide access to remote databases used for offering such services as National 800 Number. Some of the intelligence which would normally reside in a local switching office is now removed and concentrated at a distant point reached by the packet-switched network. There are only a few of these databases, and they are another source of major vulnerability (from accidental or intentional destruction of software data stored in the databases).

I should note that the enormous proliferation of private networks will not alleviate these problems. Such networks employ the same technologies, and unless they are interconnected and interoperable with the public networks they do not provide much redundancy. Indeed, many of these network lines interconnect with the public networks through hubs like Hinsdale, and often their lines are laid along the same bridges and highways as the public network lines. In any event, private lines between business offices will not help a resident who needs immediate access to 911 service after a central office burns down.

D. Remedial Steps

What needs to be done? As I indicated earlier, our Committee's full report will be published this Spring. Here I would like to highlight for you some of the Committee's recommendations for enhancing the NSEP capabilities of the public switched networks. I will emphasize those recommendations which speak to the role that the federal government can play in this remedial process.

Government must be able to analyze what network features are necessary for national security. Government must also be able to implement plans and procure services pertinent to national security needs. In its efforts to date to evaluate the NSEP capabilities of the public networks the federal government has not considered how network capabilities might be enhanced to reduce vulnerabilities to broader economic and social disruption. There is a gap in NSEP oversight: our Committee believes that the government should review whether its existing resources are sufficient to adequately perform expanded NSEP oversight of the proliferating public networks, and clarify the appropriate agency missions to address these broader NSEP questions.

Next, trends in technology are increasingly concentrating public network assets in a few dominant technologies which I have discussed today: fiber, digital switching and software. The Committee finds that these trends could adversely affect NSEP, and recommends action to make critical network nodes more secure, reduce the concentration of network traffic, and examine ways to provide more diversity in transmission facilities.

A third vital step to enhance NSEP is to augment existing crisis management capabilities. For emergency services to be efficiently delivered it is important to plan ahead: the day after an earthquake is no time for original research in crisis management. The government should establish additional emergency plans, tailored to the evolving public networks, which use simulated disaster and recovery scenarios to develop fallback strategies for network use during emergencies, for example, protection and backup of vital network nodes.

Perhaps the most disturbing of the growing network vulnerabilities is that of increasingly open outside access to network databases. The desire to open access to the public networks must be counter-balanced by a recognition that the integrity of the public networks must be protected. The government should address how to protect the public networks from penetration by hostile users, especially with regard to harmful manipulation of any software embedded within the public networks which is open to customer access for purposes of network management and control.

We will make these and other recommendations in our Phase II report to our sponsor, the NCS. We will not make specific recommendations as to how they should be implemented, as such advice would go beyond the Committee's charter.

E. Conclusion

In conclusion, the public networks are becoming more vulnerable to serious disruption. Recent events such as the Hinsdale fire demonstrate the increase in magnitude of service outages. The ARPANET computer worm graphically demonstrates the growing potential for misuse of our communications networks to damage vital software databases. In my view, these events could be but the tip of the iceberg, harbingers of even more serious disruptions that could occur in the 1990s.

The vulnerabilities stemming from network technology are not significantly offset by any counter-trend. Robust systems such as NETS will be necessary to enable the government to carry out vital NSEP responsibilities. Civil emergencies will also require enhancements and back-up to the capabilities of networks whose architectures are being driven primarily by economic incentives rather than by security concerns.

As I noted earlier, our Information Society is increasingly dependent on the smooth functioning of our information highways. Residential users need 911 service and will increasingly rely on "smart home" data services, such as alarm monitoring and energy management; business users--notably, the international financial community-- cannot run their enterprises without enormous volumes of voice and data services; and thus the same concerns apply for government users.

I believe that we must act now to reduce the network vulnerabilities I have described in my testimony. I have today cited some of our Committee's major recommendations for enhancing emergency service capabilities to the public switched networks. Other recommendations are presented in the Committee's forthcoming report, and if it pleases the Committee I will be happy to provide copies of the full report as soon as they are available. Critical to the effectiveness of our report and its recommendations is a sense of urgency which I hope these hearings and your Committee may help instill.

Again, I thank you, Mr. Chairman and the members of the Committee, for your interest and for this opportunity to testify here today.

TESTIMONY OF THE
NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

Pursuant to a request from the Honorable Senator John Glenn, Chairman of the United States Senate Committee on Governmental Affairs, the National Security Telecommunications Advisory Committee (NSTAC) provides this testimony regarding the effectiveness of the NSTAC. This testimony first examines the background, purposes, and organization of the NSTAC. Then, the accomplishments of NSTAC are discussed. Finally, the NSTAC's current undertakings and initiatives are explored.

I. Background, Purposes, and Organization

In 1982, recognizing the diverse structure of the telecommunications industry that provides national security emergency preparedness (NSEP) telecommunications services (and anticipating the Bell System divestiture), as well as the need for cooperation among industry participants in meeting NSEP needs, President Reagan formed the NSTAC. Established by Executive Order 12382, dated September 13, 1982, the NSTAC provides expert advice and assistance to the President. Pursuant to that Executive Order, the NSTAC is composed of up to 30 members, appointed by the President from the senior executive ranks of the nation's leading telecommunications companies. (The companies presently represented on the NSTAC are set forth in Attachment 1.)

The NSTAC provides the telecommunications industry's perspective on the survivability of NSEP telecommunications services and suggests enhancements where appropriate. In its endeavors, the NSTAC is supported by an Industry Executive Subcommittee (IES), which consists of an executive appointed from each NSTAC company. The IES establishes industry task forces and working groups to pursue issues of particular NSEP telecommunications interest or concern.

The specifically enumerated functions and duties of the NSTAC, as set forth in Executive Order 12382, are to provide to the President, among other things, (1) information and advice with respect to the implementation of national security telecommunications policy, (2) information and advice regarding the feasibility of implementing specific measures to improve the telecommunications aspects of the U. S. national security posture, and (3) technical information and advice in the identification and solution of problems which the NSTAC considers will affect national security telecommunications capability.

In carrying out its functions and duties, NSTAC is also to conduct reviews and assessments of the effectiveness of national security telecommunications policy. The NSTAC periodically reports to the President and to the Secretary of Defense (in his capacity as Executive Agent for NCS) regarding these matters. (The relationships between and among the NSTAC and various governmental entities are set forth in Attachment 2.)

The NSTAC is designed to serve, and indeed does serve, as the government's link to the telecommunications industry with respect to NSEP telecommunications. It also provides a forum for joint industry-government national security telecommunications planning. In its designed role, the NSTAC has developed recommendations to the President in a number of key NSEP areas, including: national coordination of emergency responses; commercial satellite survivability; commercial network survivability; automated information processing; and electromagnetic pulse effects.

II. Accomplishments

The NSTAC has accomplished many things with respect to a number of major NSEP issues. Seven such issues are not being analyzed by active NSTAC forums at this time, but the relevant forums with respect to five of the issues can be reactivated if necessary. Those issues are: (1) Automated Information Processing; (2) Commercial Network Suvivability; (3) Electromagnetic Pulse; (4) Funding of NSTAC Initiatives; and (5) Industry Information Security. The two remaining issues not currently being analyzed will not be revisited because their assessment by the NSTAC is complete. Those issues are : (1) International Diplomatic Telecommunications; and (2) the National Coordinating Mechanism.

National Coordinating Mechanism

As a result of the Federal Communications Commission's Computer Inquiry II decisions and the divestiture of the Bell Operating Companies from AT&T, the federal government no longer had a de facto single manager for end-to-end telecommunications services. Thus, one of the first issues considered by the NSTAC was the ability to coordinate the response of the various telecommunications vendors and carriers in the event of an emergency situation.

In July 1982, a National Security Telecommunications Conference attended by senior industry and government representatives gave priority to joint network planning. At the inaugural meeting of the NSTAC in December 1982, the National Coordinating Mechanism (NCM) Task Force was established. That task force addressed the need to coordinate and link the operations centers of major telecommunications carriers with the government's operation centers. The NSTAC recommended to the President that priority be given to creating a mechanism for reconstitution of telecommunications capabilities in case of emergencies. The resulting mechanism would be the center of the nation's capability to harness telecommunications in response to any national crisis.

As noted above, the Modified Final Judgment (MFJ) entered in the AT&T antitrust litigation separated the Bell Operating Companies from AT&T. The MFJ recognized that the continued provision of telecommunications service to the government for national security was essential even after divestiture. The MFJ therefore mandated that AT&T continue to provide, and that the Bell Operating Companies establish, a single point of contact for the provision of NSEP telecommunications.

National Coordinating Center

Building upon this framework, the NCM Task Force recommended initiatives that included the establishment of a joint industry-government National Coordinating Center (NCC). (The organization of the NCC and its present membership are set forth in Attachment 3.) The mission of the NCC is to assist in the initiation, coordination, restoration, and reconstitution of NSEP telecommunications services or facilities. That mission is accomplished through a unique organization staffed, operated, and funded by both the federal government and private industry. The goal of the NCC is to assure that the nation's telecommunications resources are available under all emergency conditions, including war.

The NCC is staffed by representatives of both telecommunications companies and federal agencies having major telecommunications assets. The representatives assigned to the NCC are knowledgeable of their company's or agency's system. In an emergency or crisis situation, the NCC will determine the extent of damage and the steps necessary to restore telecommunications services. In this regard, each representative maintains lists of contacts within the parent organization in order to know whom to call on, as well as an inventory of equipment available for emergency use.

In addition to their coordinating mission, NCC representatives work together on a day-to-day basis to prepare plans and procedures to deal with major disasters and emergencies ranging from fires, floods, and earthquakes, to a nuclear attack on the United States. The industry representatives work with the government representatives to determine which essential government telecommunications services can be restored and the priority of each. That mutual effort will result in more efficient and rapid restoration of telecommunications than if the government dealt individually with each company.

Implementation of the NCC was effected one year after the NSTAC's inaugural meeting. This demonstrates how industry and government, working together, can be responsive to the nation's telecommunications services needs in the post-divestiture environment.

In some ways, the NCC is akin to a fire department. The firefighters, while waiting for an alarm, examine potential emergencies and plan how best to respond to them. In day-to-day operations, the NCC facilitates the rapid exchange of information to deal promptly with telecommunications emergencies and crises.

The NCC has responded during real emergencies such as Hurricane Gilbert, the Cuban prisoner riots, the fires in the Brooklyn, New York and Hinsdale, Illinois central offices. It has also supported the U.S. Customs Service and the U.S. Coast Guard in drug interdiction efforts in south Florida, and has operated during the earthquakes in Coalinga and Palm Springs, California.

The Hinsdale, Illinois fire on May 8, 1988 is a recent example of an NSEP restoration effort. This occurrence was well documented by the Office of the Manager, NCS in a report entitled May 8, 1988, Hinsdale Telecommunications Outage. That report notes that the NCS/NCC supported restoration activities by facilitating coordination between affected NSEP users and telephone service providers. The NCC also took NSEP action to assist restoration of telecommunication services supporting the national power grid.

In the Hinsdale occurrence, several Federal Government agencies, including the Federal Aviation Administration, Veterans Administration, Department of Commerce, NRC, DOE, and GSA, experienced service interruptions of different magnitudes. Because no special assistance was requested by designated authorities, and only one NSEP action was initiated by the NCC, the Hindale outage was not considered a major NSEP "telecommunications emergency."

NCC member companies have also supported certain Presidential and Department of Defense telecommunications requirements, including the provision of communications for U. S. and Soviet inspectors under provisions of the INF Treaty.

That the industry members of the NCC provide representation at their own expense is noteworthy. If the situation warrants the addition of supplemental industry personnel to support the NCC, any added expense is paid by the government.

International Diplomatic Telecommunications

On September 27, 1983, in response to a request to advise the Department of State on the vulnerability and risks inherent in overseas leased networks, the IES formed the International Diplomatic Telecommunications (IDT) Task Force. In April 1984, the NSTAC forwarded two IDT recommendations to the President: (1) review vulnerabilities and risks at overseas diplomatic posts using guidelines developed by the IDT Task Force; and (2) establish a Department of State point-of-contact to serve the telecommunications needs of foreign missions operating in the U.S. Relatedly, the NSTAC also instructed the IES to assist the Department of State in determining the feasibility of using U.S. industry-owned telecommunications resources to support diplomatic requirements during international crises.

Like the NCM Task Force, the IDT Task Force has been dissolved because its specific assessment responsibilities were met.

Automated Information Processing

The need to ensure a survivable automated information processing (AIP) capability to support NSEP telecommunications prompted the NSTAC to initiate a study of AIP on December 14, 1982. The AIP Task Force assessed the issue for nearly two years.

In July 1983, April 1984, and December 1984, the NSTAC forwarded AIP recommendations to the President regarding, among other things, the need to establish a full-time management entity to implement the telecommunications AIP survivability effort.

Commercial Network Survivability

On February 29, 1984, the IES initiated the assessment of the commercial network suvivability (CNS) issue. It formed the CNS Task Force and instructed that body to identify ways to improve the survivability of commercial communications systems.

In October 1985, the NSTAC made five CNS recommendations to the President, including recommendations regarding the specification of survivability requirements for NSEP services and the development of NSEP network architecture plans.

Electromagnetic Pulse

In response to a government request, in September 1983, the IES initiated a study of the electromagnetic pulse (EMP) survivability of the national telecommunications networks. In December 1984, the NSTAC made three EMP recommendations to the President: (1) designate an appropriate federal agency to serve as an industry point-of-contact for EMP matters; (2) support industry through its standard-setting organizations in the development of electromagnetic standard that take EMP issues into account; and (3) undertake a program to improve the EMP endurability of the nation's commercial electrical power systems.

Funding of NSTAC Initiatives

In April 1984, the NSTAC agreed to assess the Funding of NSTAC Initiatives (FNI) so as to fulfill the need for cost-benefit information regarding its recommendations. Seven months later, the NSTAC followed the FNI Task Force's direction and instructed the IES to adopt the funding methodology developed by that task force, issue it as guidance to all extant and future task forces, and direct those task forces to provide cost, benefit, and funding mechanism information for each initiative recommended.

Industry Information Security

Because of concern within both industry and government regarding the protection of sensitive but unclassified information, the President asked the NSTAC to identify initiatives to protect such information. In August 1986, the IES formed the Industry Information Security (IIS) Task Force, which defined sensitive information and categories of same, the relationships between telecommunications and automated information systems, an analytical methodology, and proposed areas for further assessments. In 1988, the NSTAC made eight IIS recommendations to the President, all drawn from the IIS Task Force's final report.

III. Current Undertakings and Initiatives

The NSTAC is currently assessing six issues in active task forces or working groups. Those issues are: (1) Commercial Satellite Survivability; (2) Telecommunications Systems Survivability; (3) Telecommunications Industry Mobilization; (4) Telecommunications Service Priority; (5) National Telecommunications Management Structure; and (6) Energy.

Commercial Satellite Survivability

The ability of commercial satellite carriers to provide telecommunications support to NSEP users during emergency situations is critical to national level emergency planning. The government is implementing the Commercial SATCOM Interconnectivity (CSI) program to ensure that that support is provided. Rapid changes in satellite technology, the need to provide for international connectivity, and diverse NSEP user requirements require a periodic reassessment of the program's goals and options. The government requested that the NSTAC's Commercial Satellite Survivability (CSS) Task Force review and provide advice concerning the government's CSI Phase II program.

Thus, the NSTAC CSS Task Force is assisting in the government's CSI Program by (1) reviewing the implementation of initiatives and objectives established by the Phase II Architecture, and (2) offering recommendations based on achieving these initiatives and objectives given any change in technology that has an impact on commercial satellite survivability. In this way, the CSS Task Force will assess the technical, operational, and international implications of commercial satellite capabilities for application to the improvement of the nation's NSEP telecommunications posture.

Telecommunications Systems Survivability

The Telecommunications Systems Survivability (TSS) Task Force, composed of IES members or their representatives, is to provide a continuing review of government actions on past NSTAC recommendations. The NSTAC has made a series of recommendations to the President which relate to survivability. These recommendations are in the areas of Commercial Network Survivability (CNS), Electromagnetic Pulse (EMP), Commercial Satellite Survivability (CSS), National Coordinating Mechanism (NCM), and Automated Information Processing (AIP). In addition, the task force conducts studies of new technologies. At its February 18, 1987 meeting, the NSTAC charged the TSS Task Force to assess the impact of new technologies on survivability issues.

More specifically, the TSS Task Force has been asked to: (1) continue review of NSTAC task force studies/recommendations and government actions; (2) continue study of new technologies' applicability to the survivability of NSEP telecommunications; (3) establish a network management subgroup to assist the government in implementing the NSTAC's network management recommendations; (4) review the government's request for assistance in developing a government-wide approach for obtaining essential service protection; and (5) develop recommendations to the NSTAC on the above items.

As a result, the TSS Task Force intends to : (1) evaluate the overall progress and direction of government and industry telecommunications systems survivability efforts on a periodic basis; (2) identify new technologies and specific applications of those technologies that can be applied for the enhancement of the survivability of NSEP telecommunications with the approval of the IES; (3) establish an interim network management subgroup to assist the government in the implementation of the joint group contract effort; and (4) provide advice to the government on guidance developed for government agencies for the procurement of essential service protection.

Telecommunications Industry Mobilization

The capability to mobilize and use the nation's telecommunications resources to meet national security needs is a vital national concern. Telecommunications in the U. S. are supplied predominantly through the private sector. The telecommunications industry thus plays a critical role in ensuring the nation's ability to mobilize its resources effectively. The participation and commitment of the telecommunications industry are, along with leadership and support from the federal government, essential for effective telecommunications mobilization planning and preparedness.

The Telecommunications Industry Mobilization (TIM) issue was first focused upon by a NSTAC TIM Task Force. As a result of a recommendation of that task force, a joint industry-government TIM Group was established by and reports to both the NSTAC and the NCS Committee of Principals. The following seven mobilization subjects were identified for study: (1) personnel issues; (2) telecommunications service surge requirements; (3) government and industry mobilization management structure; (4) dependence on foreign sources; (5) dependence on other infrastructure systems; (6) maintenance of stockpiles and inventories; and (7) jurisdictional issues (federal, state and local).

The joint industry-government TIM Group was established to assist the NCS and the National Security Council in both identifying possible impediments to effective telecommunications industry mobilization and mobilization planning, and developing corrective actions to overcome any identified impediments. The current TIM effort was conceived as a three-year project, and is now in its third year.

Telecommunications Service Priority

The Telecommunications Service Priority (TSP) System is a priority system for the nation's most important NSEP telecommunications services. The TSP System authorizes and requires telecommunications vendors to both provide new NSEP services and to restore existing NSEP services before all others. The TSP Task Force is to assist the NCS as it implements the TSP System by making recommendations for those aspects of the TSP System most directly affecting the telecommunications industry.

Since 1967, the NCS has administered the Restoration Priority (RP) System. Vast changes in the telecommunications industry, along with problems with administering the RP System, have created a need to implement a more modern system. The TSP System was developed both to address these problems and to take advantage of emerging technology. On November 17, 1988, the Federal Communications Commission authorized the TSP System. National Security Emergency Preparedness Telecommunications Service Priority, Report and Order, FCC 88-341, released November 17, 1988.

The TSP Task Force continues to provide advice and assistance to the NCS in conceptualizing and designing a system setting priorities with respect to the initiation and restoration of NSEP telecommunications. The task force's intent is to assist the NCS in developing a system that is not only fully responsive to NSEP requirements, but which also minimizes the impact on internal company operations, ensures effective system administration, and recognizes the varying requirements of TSP service users.

National Telecommunications Management Structure

A National Telecommunications Management Structure (NTMS) is required to support NSEP telecommunications requirements in the event of national emergency and/or nuclear war. At its November 6, 1987 meeting, the NSTAC recommended that the President approve the NTMS Implementation Concept. The President subsequently approved the concept for implementation, and a trial exercise held July 12-15, 1988 demonstrated the viability of the concept.

The NTMS Task Force is to continue to serve, in conjunction with the NCC, as the planning forum for NTMS, and will provide final trial results and implementation progress at the next NSTAC meeting. The task force will strive to resolve future industry-government commitment and funding issues, identify NTMS site locations, and assist in both the development of the National Telecommunications Coordinating Network (NTCN) Architecture and in achieving NTMS initial operating capability in the mid-Atlantic region.

Energy

At its February 18, 1987 meeting, the NSTAC recommended that the President initiate a study to identify options for ensuring the survivability of power as it relates to telecommunications. The NSTAC also offered its services to support the effort. Energy and telecommunications are and will remain highly interdependent and, thus, are critical to NSEP.

In accordance with the IES's direction, the NSTAC Energy Task Force will advise the government in its efforts to implement the NSTAC's electric power recommendation. It is anticipated that the Energy Task Force will: (1) develop recommendations to mitigate the effects of electric power vulnerabilities affecting telecommunications; (2) develop recommendations to the government for establishing a priority mechanism for electric power and fuel distribution under emergency conditions; and (3) work with the Department of Energy both to determine the nature and extent of the interdependencies of telecommunications and electric power and to develop recommendations to mitigate any deficiencies resulting from such interdependencies.

Conclusion

The NSTAC, in its more than six years of existence, has proven to be an outstanding example of how industry and government can cooperate effectively to address issues of utmost importance to the nation. The process by which the NSTAC advises the President with respect to the implementation of national security telecommunications policy and related matters functions well.

As evidenced by both its activities to date and its current initiatives, the NSTAC provides important input with respect to the continuing enhancement of national security emergency preparedness telecommunications. Perhaps more importantly, the NSTAC stands prepared to address, in a timely and effective manner, new initiatives and issues in its area of expertise and responsibility. In the event that this Committee or any other government or industry body believes such an issue needs to be addressed, but has yet to be, the NSTAC urges that the issue be brought to the attention of the President for treatment by NSTAC.

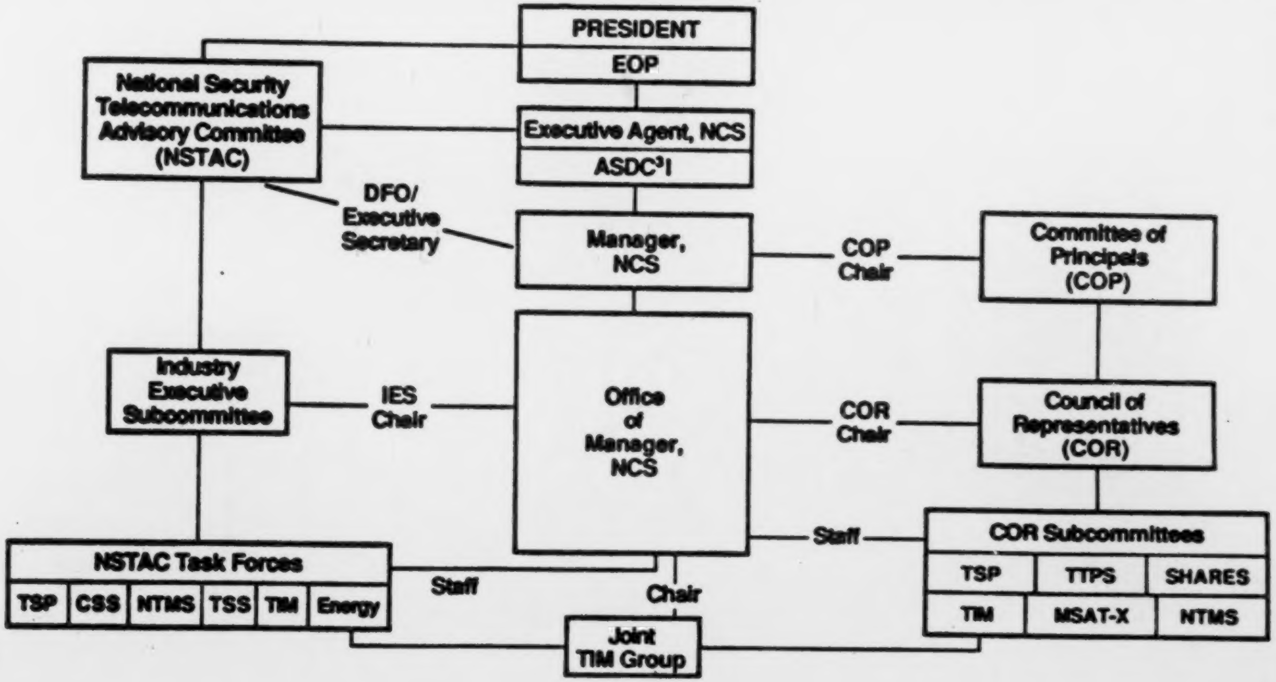
In sum, the NSTAC is functioning well and welcomes increased use. A recent survey of the NSTAC's members showed that the telecommunications industry participants believe that the NSTAC's work should continue unabated. Moreover, in a letter dated July 11, 1988, President Reagan praised the NSTAC and urged his successor to continue utilizing the NSTAC with respect to these vital national security concerns. The NSTAC firmly believes that the President should do so in order to address these important matters.

NSTAC members include senior executives from:

- AT&T
- Bell Communications Research, Inc.
- The Boeing Company
- Communications Satellite Corporation
- Computer Sciences Corporation
- Contel Corporation
- Control Data Corporation
- Fairchild Industries
- Ford Aerospace Corporation
- General Electric Company
- GTE Corporation
- Harris Corporation
- Hughes Aircraft Company
- IBM
- ITT Corporation
- Lockheed Corporation
- Martin Marietta Corporation
- McCaw Communications Company
- McDonnell Douglas Corporation
- MCI
- Motorola, Inc.
- Northern Telecom, Inc.
- Pacific Telecom, Inc.
- Rockwell International Corporation
- TRT Telecommunications Corporation
- Unisys Corporation
- United Telecommunications, Inc.
- U.S. Telephone Association

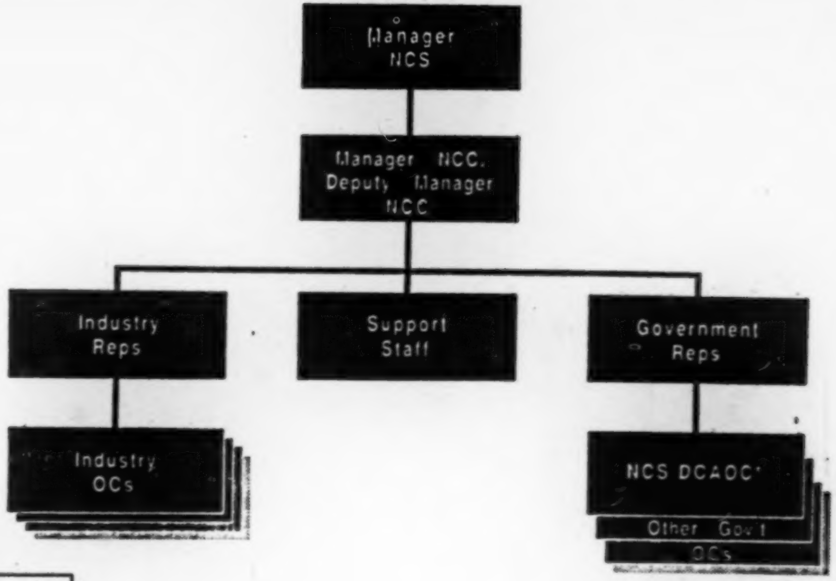
ATTACHMENT 1

Joint Industry – Government Structure


PRESIDENT
EOP
National Security Telecommunications Advisory Committee (NSTAC)
Executive Agent, NCS
ASDC³I
DFO/ Executive Secretary
Manager, NCS
COP Chair
Committee of Principals (COP)
Industry Executive Subcommittee
IES Chair
Office of Manager, NCS
COR Chair
Council of Representatives (COR)
Staff
COR Subcommittees
TSP
TTPS
SHARES
TIM
MSAT-X
NTMS
NSTAC Task Forces
TSP
CSS
NTMS
TSS
TIM
Energy
Staff
Chair
Joint TIM Group

ATTACHMENT 2

NCC Organizational Structure



Manager NCS

Manager NCC, Deputy Manager NCC

Industry Reps

Support Staff

Government Reps

Industry OCs

NCS DCAOC*

Other Gov't OCs

- ▬ Operational Support
- ▬ Coordination/Guidance
- ▬ Direction/Control

*Operational Facility Support to NCC

ATTACHMENT 3 (1)

The following companies are members of, and provide employees to staff, the NCC:

AT&T
Bell Communications Research, Inc.
Contel Corporation
General Electric Company
GTE Corporation
ITT Corporation
Martin Marietta Corporation
MCI
Pacific Telecom, Inc.
TRT Telecommunications Corporation
U.S. Telephone Association

ATTACHMENT 3 (2)

STATEMENT OF BENHAM E. MORRISS

DEPUTY MANAGER

NATIONAL COMMUNICATIONS SYSTEM

Mr. Chairman and Members of the Subcommittee:

I am pleased to appear in response to your request to discuss the National Communications System's emergency preparedness programs designed to prevent or to respond to major interruptions in national security emergency preparedness (NSEP) telecommunications capabilities which may occur in a peacetime environment. NSEP telecommunications services are:

> those telecommunication services which are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) which causes or could cause injury or harm to the population, damage to or loss of property, or degrades or threatens the NSEP posture of the United States.[1]

The NCS is not charged with ensuring that every business or residential subscriber has telephone service during a disaster or emergency. The focus is on ensuring that telecommunications are available to Federal agencies, and in some cases to state and local agencies as well, that are charged with responding to or managing such events or crises.

The National Communications System (NCS) was established in 1963 by President John F. Kennedy as a result of shortcomings in emergency communications identified during the Cuban Missile Crisis in October, 1962.[2] The NCS was charged with providing necessary communications for the Federal Government under all conditions ranging from a normal situation to national emergencies and international crises, including nuclear attack. This mission was further defined by both President Carter and President Reagan to include major disasters, national mobilization, intelligence activities, diplomacy, continuity of government, conventional war, nuclear attack and postwar recovery. Thus, the NCS has planning responsibility to ensure that

---

1. This definition of NSEP telecommunication services was approved by the National Security Advisor to the President, with his approval of the NSEP Telecommunications Procedures Manual, and by the Federal Communications Commission in its Telecommunications Service Priority System, 47 CFR Part 64.401, Appendix.

2. The original concept of a national communications system, which was envisioned by President Kennedy as a single government system, was never achieved. Rather, as confirmed by Exec. Order No. 12472, 49 Fed. Reg. 13471 (1984), reprinted in 50 U.S.C.A. App § 2251 at 296 (West Supp. 1988), what has evolved is a consortium of Federal Agencies with telecommunication systems and assets that are significant to national security and emergency preparedness. This consortium is directed, among other things, to ensure that the collective assets are responsive to the NSEP needs of the President and the Executive branch; capable of satisfying priority telecommunications requirements under all circumstances; and, incorporate the necessary combination of hardness, redundancy, mobility, connectivity, interoperability, restorability and security to obtain, to the extent practicable, the survivability of NSEP telecommunications.

NSEP telecommunications are available to the Federal Government to respond to incidents which occur in a peacetime environment such as terrorist acts, sabotage, or natural disasters.

Federal Agency Cooperation

The NCS administrative structure directly supports its vital mission of coordinating the planning for the provision and restoration of NSEP telecommunications. The Secretary of Defense serves as NCS Executive Agent, while the Director of the Defense Communications Agency is the Manager, NCS. The NCS Committee of Principals - composed of senior representatives from each of the 23 NCS member organizations - is the NCS central body. The committee serves as a forum to deliberate NCS activities and to make recommendations regarding NSEP telecommunications issues to the Executive Agent and Manger, NCS, as well as to the Office of Science and Technology Policy,[3] Office of Management and Budget and National Security Council.

The Manager, NCS, is charged with developing a recommended evolutionary NSEP telecommunications architecture; developing plans and procedures for the management, allocation and use of federal telecommunications assets under all emergency or crisis conditions; developing plans, procedures and standards that facilitate interoperability; conducting test and exercise programs and procedures; and developing alternative mechanisms for funding NSEP telecommunications initiatives.

Government and Industry Partnership

Because the Federal Government relies on commercial communications for nearly all of its service needs domestically and procures telecommunications equipment from multiple commercial vendors, government and industry are linked inextricably in the mission to provide effective NSEP telecommunications.

To obtain the telecommunications industry's assistance in implementing NSEP telecommunications policy, particularly in light of the development of competition in the industry and the divestiture of the Bell Operating Companies, President Reagan created the National Security Telecommunications Advisory Committee (NSTAC) consisting of senior representatives from up to 30 major U.S. telecommunications and information processing companies. NSTAC provides advice and assistance to the President on technical and policy issues to enhance NSEP telecommunications.

The 1980s have been a decade of intense government and industry cooperation for the betterment of NSEP telecommunications. President Reagan recently commended NSTAC for "its continuing, dedicated support of our telecommunications objectives for national security emergency preparedness," and he referred to NSTAC's work as an "unmatched record of sustained effort and accomplishment ."

---

[3] Pursuant to Exec. Order No. 12472, OSTP is directed to provide information, advice, guidance and assistance, as appropriate, to the President and to those Federal departments and agencies with responsibilities for the provision, management, or allocation of telecommunications resources, during non-wartime crises or emergencies.

Vulnerability of the Nation's Telecommunications Resources

Major disruptions of the nationwide telecommunication networks during a peacetime emergency or disaster would be highly unlikely. The individual networks have diverse, robust and redundant transmission facilities and switching capabilities which enable them to reroute traffic or restore facilities with very limited loss of telecommunications capability. This results in part from the variety of transmission facilities used in interexchange communications which include domestic satellite, microwave, fiber optic and analog cables. Absent a major regional disaster, such as an earthquake or hurricane, regional telecommunications share the same diverse, robust and redundant facilities and are similarly protected from major disruption from isolated incidents. The availability of alternative interexchange service providers, as a result of the introduction of competition to the telecommunications industry, has enhanced the diverse and redundant character of interexchange communications. Even incidents involving a single local exchange area, while having potential for serious disruption of services within that local exchange area, are minimized for those government agencies and businesses which access interexchange carrier facilities through private facilities designed to bypass the local exchange carrier facilities.

Last year's fire at a major, or gateway, Illinois Bell switching facility at Hinsdale, Illinois, exemplifies the role of the NCS in restoring emergency communication. On May 8, 1988, the fire damaged 8,718 carrier systems and 432 fibers in six cables at the Hinsdale switching facility. The fire caused loss of service and isolation for 35,000 customers in Chicago's western suburbs, some of whom did not regain full, reliable service until June. Nonetheless, except for calls destined for the Hinsdale service area, the rest of the nationwide network was unaffected. Long distance calls were routed around the Hinsdale facility. Even within the Hinsdale service area, some customers utilized bypass facilities which provided a separate access to the nationwide public switched network.

Although the fire was not considered a major NSEP emergency, partly due to network's alternate routing and bypass capacity, the NCS facilitated the restoration of communication services to critical public and private users in the area. The Federal Aviation Agency, the Veteran's Administration, the Nuclear Regulatory Commission and the Department of Commerce sustained some disruption due to the fire and requested restoration of their priority services. Although we cannot ascertain whether service restoration always was accomplished in accordance with the procedures of the existing Restoration Priority system, priority services appear to have been restored relatively quickly. For instance, the FAA reported no significant impact to air traffic in the Chicago area after the first two days. The NCS also assisted in the restoration of various MILNET circuits from the Argonne National Laboratory (a Department of Energy (DoE) facility) to five Department of Defense installations in four states. Some problems experienced by the Veteran's Administration in the identification of its priority circuits should be cured with implementation of the TSP system.

It is important to note that the NCS, and the National Coordinating Center (NCC) which the NCS operates and which is addressed later, while not responsible for all telecommunications services in an area, does facilitate restoration of emergency services beyond those of federal agencies. In this instance, the Hinsdale fire also disrupted services for the North American Electrical Reliability Council (NAERC) Coordination Center. Working with the DoE, the NCC was able to identify NAERC circuits which were critical to the monitoring and management of the power grid of the continental United States. The NCC determined these commercial circuits would have qualified for assignment of restoration priorities had they been submitted to the FCC by an appropriate Federal sponsoring agency. Therefore, the NCC accelerated restoral actions by authorizing the carrier to proceed with priority restoration of these circuits.

NCS Programs and Plans In Place

Notwithstanding the strengths of the nationwide telecommunication networks, the NCS, has been tasked to ensure that nation's telecommunications resources: a) are responsive to the NSEP needs of the President and the Federal departments, agencies and other entities; b) are capable of satisfying priority telecommunications requirements under all circumstances through use of commercial, government, and privately owned telecommunications resources; and c) incorporate the necessary combination of hardness, redundancy, mobility, connectivity, interoperability, restorability and security to obtain survivability of NSEP telecommunications in all circumstances.[4] With the advice and assistance of the NSTAC, the NCS is pursuing programs in accord with these taskings which will further enhance the survivability of these networks and their ability to respond to emergency situations.

National Coordinating Center

One of the first issues addressed by NSTAC was the need for a national coordinating mechanism for operational management of NSEP telecommunications. The National Coordinating Center (NCC) was created to answer this need, and it initiated operations on January 3, 1984, in NCS headquarters. Its mission is to assist in the initiation, coordination, restoration and reconstitution of NSEP telecommunication services or facilities. The NCC is not intended to be the initial step for assistance in the provisioning (installing new services) or restoration (curing interruptions of existing services) of NSEP telecommunications services; NCC assistance is a last resort after normal contacts have been exhausted. NCC practices government-industry cooperation daily as government representatives work with personnel from 12 NCC-member companies to resolve telecommunications issues. The NCC functions include: a) prompt technical analysis/damage assessment of service disruptions and identification of necessary restoration actions; b) coordinate/direct prompt restoration of telecommunication services in support of NSEP needs; c) develop and exercise comprehensive service restoration plans; d) develop "watch center" type functions to work through cooperating industry operation centers to effectively monitor the status of essential telecommunications facilities; e) maintain access to an accurate inventory of the minimum essential equipment, personnel, and other resources which are available for restoration operations to include the location and capabilities of all industry's network operations centers; f) maintain ability to rapidly transfer operations from normal to emergency operations; and g) coordinate/direct network reconfiguration plans in support of NSEP needs. The member companies are AT&T; Bellcore; Communications Satellite Corporation: Contel; General Electric; GTE Corporation; ITT Corporation; Martin Marietta Corporation; MCI Telecommunications Corporation; Pacific Telecom, Inc.; TRT Telecommunications Corporation; and U.S. Telephone Association. These corporations are the primary providers of NSEP telecommunications in support of the Federal department and agencies.

---

[4] Exec. Order No. 12472, 49 F.R. 13471, (1984), reprinted in 50 U.S.C.A. App § 2251 at 296 (West Supp. 1988).

Priority Provisioning and Restoration of NSEP Telecommunications

The NCC has developed NSEP Telecommunications Procedures to permit priority provisioning of NSEP telecommunications. These procedures have been accepted by the Federal Communications Commission (FCC) as the guidelines for industry use in support of the priority provisioning of commercially-provided NSEP telecommunications service requirements.

Critical telecommunications services of the Federal Government have for a number of years been identified to the serving commercial carrier for priority restoral action. This Restoration Priority system is being revised in light of significant technological changes in the industry, and the greatly expanded number of serving carriers following divestiture. The replacing system is called Telecommunications Service Priority or TSP and will pertain to both the provisioning as well as restoration of vital telecommunication service requirements of the Federal, State, and local government. This major system improvement will become operational in 1990 and will provide the telecommunications industry with a clear picture of those existing or requested services which meet the Government's NSEP needs.

The TSP system includes two broad categories of priority service, Emergency NSEP (which requires provisioning of new services at the earliest possible time, without regard to cost) and Essential NSEP (which requires provisioning of new services by specific dates, or restoration of services promptly, normally without regard to associated overtime or expediting costs). Essential NSEP is further assigned priority levels designated "1," "2," "3," "4," or "5."

While the highest priorities necessarily involve the gravest threats to national security, they are not limited to wartime scenarios. For instance, Emergency NSEP may be provided to support federal, state or local government activity responding to a Presidentially declared disaster or emergency, or response to terrorist activity, civil disturbance, natural disaster "or any other unpredictable occurrence that has damaged facilities whose uninterrupted operation is critical to NSEP or the management of other ongoing crisis."

Other priority levels, especially Priority Levels 3 and 4 of Essential NSEP, encompass support for a wide range of state and local functions during non-wartime crises. Priority Level 3 involves threats to "Public Health, Safety, and Maintenance of Law and Order" in times of national, regional or serious local emergency. The criteria for such priority includes support for population warning, law enforcement, continuity of state and local government functions, hospitals and distributions of medical supplies, critical logistic functions and public utility services, civil air traffic control, military assistance to civil authorities, protection of critical industrial facilities and critical weather services.

Priority Level 4 involves threats to "Public Welfare and Maintenance of National Economic Posture" during any national or regional emergency. The criteria for invocation of such priority includes distribution of food, maintenance of monetary and financial systems, maintenance of price, wage, rent and salary stabilization, control of production/distribution of strategic materials and energy supplies, and prevention and control of environmental hazards or damages.

In the past, the RP system has been used to restore telecommunication services disrupted due to a wide range of causes, including natural disasters (e.g., hurricanes and floods) and civil disorders (e.g., the prison riots at federal facilities in late 1987). We anticipate the TSP system will be invoked for similar types of emergencies.

Planning for Regional Emergencies or Extraordinary Situations

The NCC maintains the National Plan for Telecommunications Support in Non-Wartime Emergencies. This plan, approved by the Executive Office of the President, serves as a basis for the planning and utilization of regional telecommunication assets and resources in support of non-wartime emergencies, including those covered by the "Robert T. Stafford Disaster Relief and Emergency Assistance Act of 1988," or in "extraordinary situations." The plan defines "extraordinary situations" to mean any "situation which, in the judgment of the FEMA Director, has unique national significance and requires coordination of the Federal presence." Such situations include "a radiological incident or disaster, catastrophic hazardous material situation, catastrophic manmade emergency, a major civil disturbance having national significance, and a response to an incident associated with a specific event such as a political, sports or entertainment extravaganza." Clearly, situations evolving from acts of terrorism would be covered.

Under the plan, the NCS relies on the resources and manpower of its member organizations to implement its plans and procedures at the field level. In anticipation of, or after, a declaration of an emergency or major disaster, or in an extraordinary situation as defined by the plan, the FEMA regional director may authorize the establishment of emergency telecommunications in the affected area in order to support federal organizations, state and local government officials and other persons involved in the recovery effort. In emergencies or major disasters, a GSA regional communicator operates as a NCS regional manager and coordinates the Federal emergency telecommunications response.

The duties of an NCS regional manager in emergencies or major disasters include (1) determination of surviving capability and required emergency telecommunications within the disaster area; (2) identification of NSEP telecommunications service requirements that must be provisioned or restored; (3) coordination with FEMA to determine telecommunication requirements to support its functions; (4) consultation with commercial carriers for telecommunications support; (5) service as the sole central telecommunications coordinating point to receive and process request for emergency telecommunications services from all Federal and major private relief organizations involved with recovery operations; (6) coordination with the

Administrator, GSA, the Manager, NCS, the Military Liaison Officer, points of contact of other NCS member organizations' regional elements, the NCC, and commercial carriers, as necessary, to satisfy requirements; and (7) coordination of the installation of all Federal Government telecommunication service requirements in the disaster area.

Federal Radiological Emergency Response Plan

The NCS is responsible for the telecommunications annexes of many other civil and military plans and procedures. It takes an active ongoing part in the planning activities of the interagency group responsible for maintaining the Federal Radiological Emergency Response Plan. This plan provides for the utilization of national telecommunications assets and resources in situations involving fixed nuclear facilities or nuclear materials - an area where the threat of terrorism is considered critical.

Joint Telecommunications Resources Board

While the NCC has the capability to coordinate Federal telecommunications support in nearly all crisis and emergency situations, there is a higher level mechanism available in situations of a magnitude well beyond the normal. The Director, Office of Science and Technology Policy, Executive Office of the President, has established a Joint Telecommunications Resources Board. The Board assists the Director, OSTP, in the performance of those non-wartime functions assigned to him in EO 12472. Major telecommunications emergencies that transcend State and regional boundaries, and/or involve a large number of Federal organizations, may be referred to the JTRB for their advice and counsel. The Board may recommend priorities, allocate or reallocate resources, and recommend appropriate action by the President. The recommendations of the Board will be carried out by the NCC and appropriate cognizant agencies.

Emergency Action Procedures

The NCS has in place emergency action procedures for alerting the telecommunications industry of changes in Federal civil and military alert conditions. Preformatted messages provide key industry officials with the opportunity to take initial precautionary measures to protect or alert their infrastructures, prior to general public notifications. In the case of non-wartime emergencies requiring the redeployment of telecommunications resources from one part of the nation to another, or from one company to another, procedures exist within the NCC for the coordination of military airlift missions, or the deployment of other pertinent military support resources.

Key Asset Protection Plans

The NCS is working closely with the Department of Defense and the Federal Bureau of Investigation as they develop programs directed at the identification of private sector facilities and services that are considered critical to our national security. These key asset protection plans, when implemented, will be the bases for joint Federal Government and private sector planning to enhance the protection of these key assets against possible acts of terrorism or war.

Participation in Exercises

The NCS and the NCC are key participants in the Federal Government's exercise program. The NCC works closely with the Department of Defense and the Federal Emergency Management Agency on planning for and implementing major national and international exercises. In the past few years, an increasing number of exercise incidents involving terrorism and sabotage have been planned and played by an expanding number of departments and agencies. The telecommunications industry members of the NCC actively participate in the planning and implementation of these exercises. Additionally, the NCC is seeking to become further involved in the special exercise programs of the Department of Energy and the Federal Bureau of Investigation. These exercises pertain directly to the implications of nuclear terrorist activities. The NCC assists Bellcore in the planning for and implementation of exercises involving all the local Bell Operating Companies. Reaction to terrorist threat/activity is a major element of this industry exercise program.

The telecommunications industry is keenly aware of the potential threat posed by terrorism. Throughout the industry employee awareness programs have been introduced. Corporate security forces and management are continually seeking ways to improve physical and information security measures. Through the NCC, the telecommunications industry keeps the Federal Government informed of service disruptions and by analysis of the information obtained from industry operating centers and Government operating centers, "patterns" can be identified. Such information is quickly shared with local, State and Federal law enforcement organizations.

NCS Programs and Plans under development

The major NCS programs and plans under development center around its three-part National Level NSEP Telecommunications Program, consisting of the Nationwide Emergency Telecommunications Service (NETS) program; the Commercial Network Survivability (CNS) program and the Commercial Satellite Communications (SATCOM) Interconnectivity (CSI) program. The National Level Program is designed to improve the connectivity and survivability of public switched networks, on which the Federal Government relies for most of its NSEP telecommunications services domestically. NSTAC provided guidance for the commercial network survivability and CSI issues, which now are formal components of the NCS National Level Program.

Nationwide Emergency Telecommunications Service

NETS will greatly increase the probability that government users will be able to communicate--even in the most catastrophic situations. NETS signaling and routing enhancements will improve the usability and flexibility of major interexchange and local exchange carrier networks. As carriers adopt economical technologies which concentrate signaling information over fewer routes, NETS enhancements diversify these routes. Through use of improved switch intelligence and deployment of call controllers, NETS expands routing alternatives for NSEP users--greatly increasing the probability of call completion. The other two programs, CNS and CSI, build upon the NETS-based commercial carrier infrastructure improvements to improve connectivity between isolated enclaves of surviving commercial carrier assets.

Commercial Network Survivability

The CNS program enhances the survivability of terrestrial networks (cable, fiber optics, microwave), including those of local exchange carrier networks by: a) Using existing government and industry mobile/transportable communications equipment for major disasters and emergencies; b) Interconnecting government and commercial carrier assets to reroute NSEP traffic; and c) Use of carrier network management techniques to provide special network handling of NSEP calls. A mobile/transportable augmentation concept was first tested in 1984, and most recently demonstrated in 1987, under a hypothetical earthquake scenario in Los Angeles, California. Using mobile military equipment to interconnect facilities of AT&T, US Sprint, General Telephone of California, and Pacific Bell, the CNS prototype successfully routed emergency calls. For the interconnect element, key candidate interconnect locations have been identified and surveys are underway to assess site feasibility and cost. The first of these will use an FAA communications link to provide back-up capability for NSEP users in the Fort Worth/Dallas area.

Commercial SATCOM Interconnectivity

Damage from natural or man-made disasters could destroy segments of the public switched network, interrupting service along affected routes. The CSI program uses satellites to make "long haul" connections and provide interoperability among different kinds of satellites and ground stations. CSI builds upon three components: interoperable satellite communication links, surviving ground-based facilities, and surviving switches. A pilot program to develop a prototype for the use of commercial satellite segments to replace or supplement damaged ground-based segments has been underway since 1987 and recently became operational. Another important aspect of the CSI program is development of interoperable telemetry, tracking, and command capabilities, a key to recovering and operating surviving satellites that belong to different carriers.

Other activities

Other current NCS activities to enhance NSEP telecommunications include the Shared Resources High Frequency Radio Program (SHARES), an evolving national high frequency network of 132 federal radio facilities; and the Mobile Satellite Experiment (MSAT-X), an ongoing feasibility assessment of mobile satellite technology for NSEP applications.

Intra-Industry Initiatives

A by-product of the NSTAC process has been coöperation within the telecommunications industry in support of NSEP telecommunications. Even as the competitive marketplace for telecommunications intensifies, NCC member companies exhibit consistent cooperation.

The commercial network survivability and Commercial SATCOM Interconnectivity programs, for example, involve the interconnection of multiple carriers necessitating cooperation between the principal participants. The development of an interoperable telemetry, tracking and command capability, which is so critical to CSI success, demands intense cooperation in the areas of design, engineering and operations.

Without the cooperation of industry representatives, major NCS-sponsored exercises to improve NSEP telecommunications would not be possible.

Such state-of-the-art technologies and services as fiber optics, photonic switching, mobile satellite communications, Integrated Services Digital Network (ISDN) and network management protocols are driving a changing network. Standards for these new technologies to ensure interoperability among telecommunications resources will require the support and cooperation of industry and government. Thus, NCS must maintain the cooperative relationship with industry that began with the NSTAC process in 1982.

Conclusion

The nation's telecommunication networks are diverse, robust and redundant, qualities which make the network as a whole very resilient. The NCS, with the advice and assistance of the NSTAC, has created a number of programs and plans that are responsive to non-wartime emergencies and disasters as well as wartime requirements which enhance the resilience of the networks. Furthermore, the NCS is currently working new initiatives which will further ensure that the nations telecommunications resources will be available during such emergencies as the telecommunication networks evolve and new technologies are developed.

This concludes my prepared statement, I am available to answer your questions.

STATEMENT OF ROBERT K. MULLEN, PH.D.

MR. CHAIRMAN AND MEMBERS OF THE COMMITTEE: I AM PLEASED TO BE BEFORE YOU TODAY TO LEND WHAT PERSPECTIVE I CAN TO THE ISSUE OF SUBNATIONAL SABOTAGE THREATS TO U.S. ENERGY ASSETS. THIS PERSPECTIVE IS DERIVED IN LARGE PART FROM DATA ACQUIRED BY ME CONCERNING ENERGY ASSET SABOTAGE WORLDWIDE OVER THE LAST THREE DECADES. THE SCOPE OF MY REFERENCE CONCERNING ADVERSARIES IS ENTIRELY SUBNATIONAL. THAT IS, I AM NEITHER CONCERNED WITH, NOR COMPETENT TO ADDRESS THREATS TO THESE ASSETS FROM SPECIAL FORCES ORGANIZATIONS OR ANY ELEMENT THAT IS ATTACHED TO THE MILITARY FORCES OF ANY NATION. SABOTAGE PERPETRATED BY INDIVIDUALS OR GROUPS NOT ACTING IN OFFICIAL CAPACITIES FOR RECOGNIZED GOVERNMENTS ARE OF INTEREST TO ME. SUCH MAY BE PERPETRATED BY THOSE TERMED TERRORISTS, INSURGENTS, CRIMINALS, EMPLOYEES, OR OTHERS NOT POSSESSING THE QUALITIES OF A NATIONAL ADVERSARY.

THE SCOPE OF MY INTEREST CONCERNING ENERGY TARGETS IS BROAD. ENERGY ASSETS TARGETED BY SUBNATIONAL ADVERSARIES INCLUDE THE PERHAPS LESS OBVIOUS SUCH AS HELICOPTERS OR AIRPLANES RENTED OR LEASED BY ENERGY COMPANIES, CONSTRUCTION EQUIPMENT USED IN BUILDING ENERGY FACILITIES, AND VARIOUS KINDS OF SUPPORT FACILITIES RELIED UPON BY THE ENERGY INDUSTRY. THE MORE OBVIOUS TARGETS AS POWERLINES, PIPELINES, ENERGY GENERATING STATIONS, AND INDIVIDUALS ASSOCIATED WITH THE ENERGY INDUSTRY, ARE OF COURSE ALSO OF INTEREST. A TABLE OF ENERGY ASSETS THAT HAVE BEEN TARGETED BY SUBNATIONALS SINCE 1980 IS APPENDED TO THIS STATEMENT.

APPENDED ALSO IS A TABLE OF THE ANNUAL INCIDENCE OF SUBNATIONAL SABOTAGE FOR EACH NATION SO AFFECTED SINCE 1980. I FEEL IT MAY BE USEFUL TO EXAMINE SOME OF THOSE SUBNATIONAL SABOTAGE ACTIVITIES AS HAVE OCCURRED OUTSIDE THE U.S. FOR A COUPLE OF REASONS. FIRST, MUCH OF THIS SUBNATIONAL ACTIVITY HAS BEEN, AND CONTINUES TO BE, QUALITATIVELY AND QUANTITATIVELY DIFFERENT FROM WHAT HAS OCCURRED AND IS OCCURRING IN THE U.S. SECOND, THERE IS CONCERN THIS COULD CHANGE.

ENERGY ASSET SABOTAGE IN SELECTED INDUSTRIAL NATIONS OUTSIDE THE U.S.

I HAVE SELECTED SEVERAL WORST-CASE EXAMPLES, IF YOU WILL, OF ENERGY ASSET SABOTAGE THAT ARE NOTABLE FOR THEIR CONSEQUENCES, POTENTIAL AND ACTUAL, AND OTHER QUALITIES. BRIEF OUTLINES FOLLOW.

BELGIUM

IN 1984-1985, THE COMMUNIST COMBATANT CELLS (CCC) CARRIED OUT A CAMPAIGN OF SABOTAGE AGAINST NATO PETROLEUM ASSETS THAT WAS CHARACTERIZED SOMEWHAT LESS BY ITS LEVEL OF INTENSITY THAN BY ITS PLANNING

AND BY ITS EFFECTIVE TARGETING OF SENSITIVE FACILITIES. BOMBINGS OF PETROLEUM PIPELINE PUMPING STATIONS AND VALVES OCCURRD AT SEVERAL LOCATIONS, AS DID BOMBINGS AND ATTEMPTED BOMBINGS OF THE PIPELINES THEMSELVES. IN NEIGHBORING FRANCE DURING THIS PERIOD, THE CCC BOMBED THE OFFICES OF THE CENTRAL EUROPEAN OPERATING AGENCY, THE NATO HEADQUARTERS FOR WARTIME PETROLEUM DISTRIBUTION IN BELGIUM, FRANCE, LUXEMBOURG, NETHERLANDS, AND WEST GERMANY.

FRANCE

TERRORIST SABOTAGE OF ENERGY ASSETS IN FRANCE HAS BEEN CHARACTERIZED BY ITS VIOLENCE. ANTINUCLEAR ENERGY EXTREMISTS HAVE ENGAGED IN TACTICS RANGING FROM ARSON AND BOMBINGS, TO THE USE OF ROCKET PROPELLED GRENADES.

SEPARATIST TERRORISTS, SPECIFICALLY THE CORSICAN NATIONAL LIBERATION FRONT (FNLC), BOMBED ENERGY ASSETS IN FRANCE IN 1985-1986, SINCE SHIFTING ITS EMPHASIS TO TOURIST TARGETS IN FRANCE AND CORSICA.

DIRECT ACTION (AD) BEGAN TARGETING ENERGY ASSETS IN 1985. IN CONTRAST TO OTHERS, THEY INCLUDED INDIVIDUALS AS TARGETS. IN 1986, AD ASSASSINATED THE PRESIDENT OF COGEMA, THE FRENCH NATIONAL NUCLEAR CONSORTIUM. PLANS TO KIDNAP AN ATOMIC ENERGY COMMISSION ENGINEER WERE CONFISCATED WHEN THE AD LEADERSHIP (INCLUDING THE INDIVIDUAL SAID TO HAVE DELIVERED THE COUP DE GRACE TO THE COGEMA PRESIDENT) WERE CAPTURED IN FEBRUARY, 1987.

SOUTH AFRICA

THE PRINCIPAL SUBNATIONAL GROUP INVOLVED IN ENERGY ASSET SABOTAGE IN SOUTH AFRICA HAS BEEN THE AFRICAN NATIONAL CONGRESS (ANC). IN 1980-1983, ANC ENGAGED IN SPORADIC CAMPAIGNS OF SABOTAGE AGAINST ELECTRICAL DISTRIBUTION SYSTEMS, AND REPEATED ATTACKS AGAINST CRUDE OIL AND COAL LIQUEFACTION REFINERIES AND PETROLEUM STORAGE DEPOTS.

THE MOST SPECTACULAR OF THESE WAS A COORDINATED OPERATION AGAINST COAL LIQUEFACTION REFINERY TANK FARMS IN SECUNDA AND SASOLBURG, AND A CRUDE OIL REFINERY AT THE LATTER LOCATION. SOME $7.3 MILLION IN DAMAGE TO PLANT AND EQUIPMENT AND LOST PRODUCTION WAS SAID TO HAVE RESULTED FROM THIS OPERATION. SINCE 1980, ATTEMPTS BY THE ANC TO SABOTAGE THESE AND OTHER REFINERIES OCCURRED IN 1983, 1984, AND 1985. NONE APPROACHED THE SOPHISTICATION AND CONSEQUENCES OF THE 1980 OPERATION.

PERHAPS THE MOST SOPHISTICATED OF ANC'S ENERGY ASSET OPERATIONS WERE THE BOMBINGS OF THE KOEBERG POWER REACTOR CONSTRUCTION SITE IN 1982. THE PRESSURE VESSEL HEADS FOR THE KOEBERG 1 AND 2 REACTORS WERE BOMBED, AS WAS CERTAIN CABLING IN THE AUXILIARY BUILDING.

FOUR EXPLOSIVE DEVICES WERE EMPLACED AND SET TO DETONATE AT INTERVALS DURING THE NIGHT OF 18-19 DECEMBER. DESTROYED WERE THE CONTROL ROD DRIVE MECHANISMS FOR REACTOR UNITS 1 AND 2: IN THE AUXILIARY BUILDING, CABLING WAS SEVERED. THIS SABOTAGE OPERATION DELAYED THE STARTUP OF THE KOEBERG REACTORS FOR ABOUT EIGHTEEN MONTHS.

SPAIN

BETWEEN 1978 AND 1982, THE BASQUE TERRORIST ORGANIZATION ETA BOMBED ELECTRICAL FACILITIES OWNED BY IBERDUERO OVER 300 TIMES, IN PART TO FURTHER THEIR CAMPAIGN AGAINST THE LEMONIZ POWER REACTOR CONSTRUCTION PROJECT. OTHER ELEMENTS OF THIS CAMPAIGN INCLUDED THREATS AGAINST WORKERS AT THE LEMONIZ PROJECT; KIDNAPPINGS AND ASSASSINATIONS OF PROFESSIONAL PERSONNEL AT THIS SITE; AND SOME REMARKABLE BOMBINGS (AS WELL AS OTHERS NOT SO REMARKABLE) ON THE SITE. ULTIMATELY, IBERDUERO CEASED CONSTRUCTION ACTIVITIES AT LEMONIZ.

ONE OF THE MOST SOPHISTICATED ACTS OF SABOTAGE AT A REFINERY ANYWHERE WAS PERPETRATED BY THE BARCELONA COMMANDO OF THE ETA IN FEBRUARY, 1987. THREE EXPLOSIVE DEVICES WERE PLACED ON A PIPERACK AT A LOCATION ROUGHLY MIDWAY BETWEEN THE REFINERY AND ITS HARBOR TERMINAL. THE DETONATIONS DESTROYED THE PIPERACK, WHICH HELD TWENTY-TWO PIPELINES THAT CARRIED EVERY PRODUCT AND FEEDSTOCK TYPE TO AND FROM THE REFINERY. AN AREA OF FORTY METERS OF PIPE WAS DESTROYED; THE TOTAL LINEAR LENGTH OF PIPE DESTROYED OR DAMAGED WAS PUT AT TEN KILOMETERS, OR SIX MILES OF PIPELINE. TOTALS OF 1,800 METRIC TONS (MT) OF CRUDE OIL (1MT = 50 BARRELS); 1,100 MT OF FUEL OIL; 500 MT OF NAPHTHA; AND VARIOUS QUANTITIES OF ETHYLENE, PROPYLENE, AND GASOLINE WERE LOST, AS WERE 10,000 CUBIC METERS OF GASES. THE REFINERY WAS SHUT DOWN FOR ABOUT THREE WEEKS. TOTAL EQUIPMENT AND LOST PRODUCTION COSTS WERE PUT AT $16 MILLION, OF WHICH $5.5 MILLION WAS DUE TO DIRECT DAMAGE TO THE PIPERACK.

A MONTH LATER, ETA ATTACKED A CAMPSA FUEL DEPOT WITH A ROCKET PROPELLED GRENADE AND SEVERAL EXPLOSIVE DEVICES, SETTING AFIRE A 260,000 GALLON DIESEL FUEL STORAGE TANK, AND DESTROYING SEVERAL TRUCKS.

WEST GERMANY

AS IN FRANCE, ENERGY ASSET SABOTAGE BY TERRORISTS IN WEST GERMANY IS OF A NATURE THAT COMPLIMENTS THE VIOLENT ASPECTS OF THEIR OTHER ACTIVITIES. INVOLVED HAVE BEEN THE RED ARMY FACTION (RAF) AND THE REVOLUTIONARY CELLS (RZ). IN 1984-1985, NATO PETROLEUM PIPELINES WERE SABOTAGED BY BOMBINGS ALMOST AS INTENSIVELY AS IN BELGIUM BY THESE GROUPS.

THE RAF HAS FURTHER BEEN RESPONSIBLE FOR THE ASSASSINATIONS OF

EXECUTIVES ASSOCIATED WITH THE NUCLEAR POWER INDUSTRY. THE LAST OF THESE, ALONG WITH THE MURDER OF A U.S. SOLDIER IN 1986, CREATED A BACKLASH AMONG THE LEFT WHO WERE OUTSIDE MAINSTREAM TERRORISM, AND WHO FELT THESE ACTIVITIES WERE COUNTERPRODUCTIVE.

AT OTHER LEVELS OF ENERGY ASSET SABOTAGE HAVE BEEN A VARIETY OF AD HOC AND EPHEMERAL GROUPS GENERICALLY TERMED 'AUTONOMOUS'. COLLECTIVELY, SOME IN THESE GROUPS OR CELLS ARE KNOWN AS 'FEUERABENDTERRORISTEN', OR 'AFTER-HOURS TERRORISTS', WHO IN 1986 SAWED DOWN OR BOMBED POWER PYLONS AND POLES WITH A FREQUENCY THAT WAS EXCEEDED ONLY IN EL SALVADOR. SOME 150 ACTS OF SABOTAGE WERE COMMITTED AGAINST THESE STRUCTURES. SOME OF THESE ACTS WERE DIRECTED AGAINST PRIMARY DISTRIBUTION LINES LEADING FROM POWER REACTORS (SPECIFICALLY, THE OBRIGHEIM, KRUEMMEL, GRUNDREMINGEN, WUERGASSEN, AND BORKEN POWER REACTORS). AS A CONSEQUENCE OF SOME OF THESE ACTS, THE POWER REACTOR REDUCED POWER, OR SHUT DOWN COMPLETELY.

AT LEAST AS STRIKING, HAS BEEN THE CAMPAIGN OF SABOTAGE AGAINST THE INFRASTRUCTURE SUPPORTING THE NUCLEAR POWER INDUSTRY. THESE ACTIVITIES, WHICH ARE THE EXPRESSION OF AN ANTI-TECHNOLOGY MOVEMENT, OF WHICH THE ANTI-NUCLEAR MOVEMENT IS A SUBSET, HAVE AFFECTED VIRTUALLY THE ENTIRE COMMERCIAL AND INDUSTRIAL INFRASTRUCTURE SUPPORTING THE NUCLEAR POWER INDUSTRY IN WEST GERMANY. CONSTRUCTION FIRMS (SOME HAVE BEEN BOMBED OR FIREBOMBED THIRTY OR MORE TIMES), TRANSPORTATION FIRMS, RAILROADS (ROLLING STOCK AND TRACK), SECURITY FIRMS, ARCHITECTURAL AND ENGINEERING FIRMS, CONSULTING FIRMS, INDIVIDUAL CONSULTANTS, BANKS AND OTHER FINANCIAL INSTITUTIONS, NUCLEAR EQUIPMENT MANUFACTURERS, SCIENTIFIC AND TECHNICAL INSTITUTIONS, AND ASSETS OF ALL KINDS OWNED BY UTILITIES THAT GENERATE POWER BY NUCLEAR MEANS ARE AMONG THOSE WHO HAVE BEEN ATTACKED BY TERRORISTS AND ANTINUCLEAR EXTREMISTS

ENERGY ASSET SABOTAGE IN SELECTED PREINDUSTRIAL NATIONS

ENERGY ASSET SABOTAGE IN PREINDUSTRIAL NATIONS, WHILE NECESSARILY DIFFERENT IN CONSEQUENCES FROM THAT IN INDUSTRIAL NATIONS IN MANY CASES, DUE IN PART TO THE PHYSICAL STRUCTURES OF THE SYSTEMS SABOTAGED, AND IN PART TO THE ENVIRONMENTS IN WHICH THEY MAY BE LOCATED, HAVE ALSO HAD CONSEQUENCES FAR BEYOND THE BORDERS OF THE NATIONS IN WHICH THE EVENTS OCCURRED.

COLOMBIA

AS OF MID-JUNE 1988, NATIONAL LIBERATION ARMY (ELN) ATTACKS ON THE CANO LIMON - COVENAS PIPELINE IN 1988 CAUSED COLOMBIA LOSSES OF $3.9 MILLION IN SPILLED CRUDE; $2.3 MILLION IN CLEANUP OPERATIONS;

AND AN ESTIMATED $50 MILLION IN LOST EXPORT REVENUE. IN 1988, THE ELN BOMBED THIS 220,000 BARREL PER DAY PIPELINE MORE THAN 50 TIMES. THIS PIPELINE AND ITS VARIOUS SUPPORT FACILITIES HAVE BEEN UNDER ATTACK BY THE ELN SINCE THE EARLY 1980'S. TO A LESSER EXTENT, ENERGY ASSETS IN COLOMBIA HAVE BEEN SABOTAGED ALSO BY THE 19 APRIL MOVEMENT (M-19), THE REVOLUTIONARY ARMED FORCES OF COLOMBIA (FARC), AND THE PEOPLE'S LIBERATION ARMY (EPL).

TARGETED ENERGY ASSETS OTHER THAN THE CANO LIMON-COVENAS PIPELINE INCLUDE A BROAD SPECTRUM OF FACILITIES AND EQUIPMENT IN THE PETROLEUM SECTOR (DRILLING AND SEISMIC RIGS, HELICOPTERS, POWER SUPPLIES, OFFICE BUILDINGS, ETC.), AND PERSONNEL. POWER SYSTEMS ARE BECOMING A MORE FREQUENT TARGET, AS ARE COAL MINING OPERATIONS, COAL MINING EQUIPMENT, AND PERSONNEL ASSOCIATED WITH COAL EXPLORATION AND MINING. PERSONNEL IN VIRTUALLY ALL POSITIONS (OIL FIELD WORKERS TO PRINCIPAL EXECUTIVES) HAVE BEEN ASSASSINATED, KIDNAPPED FOR RANSOM, OR WOUNDED DURING TERRORIST OPERATIONS AGAINST ENERGY INTERESTS.

EL SALVADOR

INSURGENTS OPERATING UNDER THE FARABUNDO MARTI NATIONAL LIBERATION FRONT (FMLN) HAVE SABOTAGED EL SALVADOR'S ELECTRICAL ENERGY ASSETS MORE PERSISTENTLY AND EFFECTIVELY THAN PERHAPS ANYWHERE ELSE. ACCORDING TO OFFICIAL SOURCES, THERE HAVE BEEN OVER 2,000 ATTACKS ON ELECTRICAL SYSTEMS BY THE FMLN SINCE 1980. THE ESTIMATED COST TO EL SALVADOR HAS BEEN $51 MILLION. WHILE POWER POSTS AND PYLONS ARE BY FAR THE MOST FREQUENT TARGETS, EL SALVADOR'S PRINCIPAL HYDROELECTRIC FACILITIES AND POWER SUBSTATIONS HAVE BEEN REPEATEDLY ATTACKED; OFTEN TO SIGNIFICANT EFFECT. WHILE EXPLOSIVE DEVICES ARE THE PRINCIPAL WEAPON OF SABOTAGE, MORTARS AND SHOULDER FIRED ROCKETS HAVE ALSO BEEN EMPLOYED AGAINST THE LARGER FACILITIES.

FMLN SABOTAGE REGULARLY RESULTS IN POWER OUTAGES OVER LARGE AREAS OF THE NATION. SUCH OUTAGES AFFECT WATER SUPPLIES AS WELL, AS WATER SYSTEM PUMPS ARE DRIVEN ELECTRICALLY THROUGHOUT EL SALVADOR.

MOZAMBIQUE

THE MOZAMBIQUE NATIONAL RESISTANCE (MNR OR RENAMO, AS IT IS KNOWN BY ITS PORTUGUESE ACRONYM), FIRST SABOTAGED ENERGY ASSETS IN MOZAMBIQUE IN SEPTEMBER, 1980: THEY BOMBED A POWER PYLON ON THE LINE FROM THE CABORA BASSA HYDROELECTRIC FACILITY IN TETE PROVINCE TO SOUTH AFRICA. BY DECEMBER, 1985, 585 OF THE 4,000 OR SO PYLONS ON THIS POWERLINE HAD BEEN BOMBED BY THE MNR. SINCE APRIL, 1988, TO THE PRESENT, OVER 900 MORE OF THESE PYLONS HAVE BEEN BOMBED. THAT IS TO SAY, SINCE APRIL, 1988, THE MNR HAS BOMBED 2-3 PYLONS PER DAY ON THE CABORA BASSA POWERLINE.

SOUTH AFRICA, TO HAVE BEEN THE PRIMARY PURCHASER OF POWER GENERATED AT CABORA BASSA, HAS RECEIVED ELECTRICITY OVER THIS POWERLINE A TOTAL OF 526 DAYS SINCE DECEMBER, 1980. THE EFFECTS OF MNR'S SABOTAGE IN THIS POWER CORRIDOR HAVE BEEN FELT NOT ONLY IN MOZAMBIQUE AND SOUTH AFRICA, BUT IN PORTUGAL AS WELL. PORTUGAL, HAVING GUARANTEED THE CONSTRUCTION BONDS FOR THE CABORA BASSA DAM, HAD INTENDED TO RETIRE THE $700 MILLION DEBT WITH THE REVENUE PRODUCED BY THE FACILITY. WHEN THIS DEBT HAD BEEN RETIRED, TITLE TO THE DAM WAS TO PASS TO MOZAMBIQUE. DUE TO MNR SABOTAGE, THE DEBT IS NOT BEING RETIRED AS ORIGINALLY SCHEDULED, AND THE PROSPECT AT THIS TIME FOR MOZAMBIQUE RECEIVING TITLE TO OR INCOME FROM THIS FACILITY IS INDETERMINATE.

MNR'S ATTACKS ON MOZAMBIQUE'S PETROLEUM INFRASTRUCTURE CONTRIBUTED TO ECONOMIC PROBLEMS IN MOZAMBIQUE, ZIMBABWE, AND MALAWI. IN 1982, THE MNR VIRTUALLY DESTROYED BY MORTAR FIRE THE PETROLEUM PRODUCT OFFLOADING FACILITIES IN THE PORT OF BEIRA. SOME THIRTY-TWO STORAGE TANKS WERE DESTROYED, LEAVING THE TERMINAL WITH INSUFFICIENT CAPACITY TO OFFLOAD SHIPS ALREADY IN PORT.

THE PETROLEUM PRODUCT PIPELINE FROM THE PORT OF BEIRA TO ZIMBABWE HAS SUFFERED A MORE OR LESS CONTINUOUS CAMPAIGN OF SABOTAGE FROM 1981 TO RECENT TIMES. THIS HAS FORCED ZIMBABWE TO IMPORT PETROLEUM PRODUCTS BY RAIL VIA SOUTH AFRICA AT SIGNIFICANTLY GREATER COST THAN BY PIPELINE. IN ADDITION, TO AID IN PROTECTING ITS INTERESTS IN MOZAMBIQUE, ZIMBABWE HAS PLACED ABOUT 13,000 TROOPS THERE AT A COST ESTIMATED TO BE $1 MILLION PER DAY.

FINALLY, THE MNR HAS VIRTUALLY SHUT DOWN MOZAMBIQUE'S ABILITY TO EXPORT COAL - FORMERLY A MAJOR SOURCE OF INCOME - BY THE SIMPLE EXPEDIENT OF BOMBING ONE RAIL LINE AND ONE BRIDGE IN TERRITORY IT FOR THE MOST PART CONTROLS. MOZAMBIQUE HAS REPORTED LOSSES IN THE COAL SECTOR OF $200 MILLION; ABOUT $80 MILLION DIRECTLY TO SABOTAGE OF EQUIPMENT AND TRANSPORTATION FACILITIES, THE BALANCE IN LOST REVENUE.

PERU

THE SENDERO LUMINOSO (SL) HAVE, SINCE 1980, CARRIED OUT A CAMPAIGN OF SABOTAGE AGAINST ELECTRICAL DISTRIBUTION AND PRODUCTION FACILITIES. THEY HAVE REPEATEDLY KNOCKED OUT POWER TO VAST REGIONS OF THE NATION; THEY HAVE DESTROYED LOCAL HYDROELECTRIC FACILITIES IN RURAL AREAS; THEY HAVE ASSASSINATED ENGINEERS AND OTHERS ASSOCIATED WITH THE PLANNING AND CONSTRUCTION OF ELECTRICAL FACILITIES; AND THEY HAVE KILLED SECURITY, POLICE, AND MILITARY PERSONNEL GUARDING ENERGY ASSETS

SABOTAGE BY THE SL HAS REPEATEDLY LEFT THE CAPITAL CITY, LIMA, WITHOUT POWER. RECENTLY, SUCH ACTIONS LEFT LIMA IN THE DARK FOR OVER A WEEK. TRAFFIC SIGNAIS, ELEVATORS, AND LIGHTING IN GENERAL DID NOT WORK; WATER PURIFICATION FACILITIES CEASED FUNCTIONING; AND REFRIGERATION BROKE DOWN EVERYWHERE IN THE CITY CAUSING FOOD TO ROT IN HOMES, STORES, AND RESTAURANTS.

SURINAME

THE RONNIEBRUNSWIJK GANG, ARMED IN PART WITH LEVER-ACTION WINCHESTERS, VIRTUALLY SHUT DOWN SURINAME'S ECONOMY IN 1986-1987 WITH A HANDFUL OF EXPLOSIVE DEVICES. THEY DID THIS BY BOMBING THE POWER SUPPLIES TO THE BAUXITE MINES IN MOENGO AND THE ALUMINA SMELTER IN PARANAM, THEN DENYING THE AREAS TO REPAIR CREWS. THE IMMEDIATE RESULT WAS TO CUT OFF SURINAME'S PRIMARY SOURCE OF FOREIGN EXCHANGE - REFINED BAUXITE ORE. A SECONDARY RESULT WAS THE SHUTTING DOWN OF THE STATE OIL ENTERPRISE. WITH THE BAUXITE INDUSTRY, IT BEING THE STATE OIL ENTERPRISE'S LARGEST CUSTOMER FOR ITS PRODUCT, IDLED, THE ENTERPRISE COULD NOT OPERATE ECONOMICALLY AT RESIDUAL DEMAND LEVELS, SO IT SHUT DOWN.

ENERGY ASSET SABOTAGE IN THE UNITED STATES

IT SHOULD BE NOTED AT THE OUTSET THAT DATA IN THE APPENDED TABLE CONCERNING ENERGY ASSET SABOTAGE IN THE U.S. INCLUDE TYPES OF INCIDENTS RARELY, IF EVER, SEEN FOR NATIONS OTHER THAN THE U.S. ACCOUNTS OF VANDALISM OR SABOTAGE COMMITTED BY EMPLOYEES OR CONSTRUCTION WORKERS AT OPERATING ENERGY FACILITIES OR FACILITIES UNDER CONSTRUCTION; HUNTERS WHO SHOOT HOLES IN PIPELINES OR SEVER POWERLINES; SHOOTINGS AT OR CONCERNING COAL MINES WHERE THERE MAY BE LABOR DISPUTES; AND THE LIKE ARE TO SOME DEGREE AVAILABLE FOR THE U.S. THIS IN GENERAL IS NOT TRUE FOR OTHER NATIONS. THEREFORE, THE TOTAL NUMBERS OF INCIDENTS NOTED FOR THE U.S. ARE NOT ENTIRELY COMPARABLE TO THOSE NUMBERS FOR ANY OTHER NATION, INSOFAR AS THE OVERALL QUALITIES OF THESE DATA ARE CONCERNED.

FOLLOWING ARE BRIEF DISCUSSIONS OF ONE OR TWO ENERGY SABOTAGE INCIDENTS IN THE U.S. FOR EACH OF THE YEARS 1980 THROUGH 1988.

1980

ON 10, 12, AND 15 FEBRUARY UNKNOWN EMPLOYEES OF THE BROWNS FERRY - 2 POWER REACTOR NEAR DECATUR, ALABAMA, CAUSED THE REACTOR TO TRIP, OR SHUT DOWN, BY MANIPULATING REACTOR CONTROL EQUIPMENT. ACCORDING TO AVAILABLE ACCOUNTS, TVA WAS REQUIRED TO PURCHASE $3 MILLION IN REPLACEMENT POWER TO COVER THE THREE OUTAGES. DURING THESE OUTAGES, THE TVA WAS ALSO LOSING REVENUE. AS A GENERAL RULE OF THUMB, THE VALUE OF THE ELECTRICITY GENERATED BY A 1,000 MEGAWATT POWER PLANT IS ABOUT $1 MILLION PER DAY. BROWNS FERRY - 2 POWER REACTOR IS RATED AT 1,067 MEGAWATTS ELECTRIC.

1980

IN FEBRUARY, PERSONS UNKNOWN PARTIALLY SAWED THROUGH THIRTY-FIVE WOODEN POLES MAKING UP EIGHTEEN 'H' FRAME POWERLINE STRUCTURES ALONG A 1.5 MILE LENGTH OF 115 KV LINE IN SOUTHWEST COLORADO. IN OCTOBER, SIXTY-THREE SUCH POLES, MAKING UP THIRTY-TWO 'H' FRAME STRUCTURES WERE PARTIALLY CUT THROUGH ALONG 3.2 MILES OF A 115 KV LINE ABOUT ONE QUARTER MILE FROM THE FEBRUARY INCIDENT. GUYWIRES TO A STRUCTURE IN THE MIDDLE OF THIS SECTION OF LINE WERE CUT, AND THE POWERLINE COLLAPSED. BOTH INCIDENTS RESULTED IN ABOUT $200,000 IN DAMAGE.

1981

IN LATE MARCH, SEVERAL SUBSTATIONS BELONGING TO A FLORIDA UTILITY WERE SABOTAGED BY RIFLEFIRE OR EXPLOSIVES. TOTAL DAMAGES WERE IN THE NEIGHBORHOOD OF $3 MILLION. OUTAGES AFFECTED SEVERAL THOUSAND RATE PAYERS FOR VARIOUS PERIODS OF TIME.

1981 - 1982

BETWEEN AUGUST AND NOVEMBER, 1981, AND APRIL 29 AND MAY 3, 1982, THERE WERE NUMEROUS BOMBINGS OR ATTEMPTED BOMBINGS OF POWER PYLONS AND SUBSTATIONS AT VARIOUS LOCATIONS IN PUERTO RICO. MUCH OF THIS ACTIVITY OCCURRED DURING LABOR DISPUTES; OTHER INCIDENTS WERE ATTRIBUTED TO THE SEPARATIST TERRORIST GROUP, MACHETEROS. DAMAGE ESTIMATES EXCEEDED $2.5 MILLION: OUTAGES TO 20,000 OR MORE RATE PAYERS SOMETIMES LASTED FOR SEVERAL DAYS.

1983

EXXON CORPORATION WAS THE OBJECT OF AN EXTORTION IN APRIL. ON 15, 18, 20, AND 28 OF THIS MONTH, THERE WERE ATTEMPTED BOMBINGS IN TEXAS AT EXXON SERVICE STATIONS. ATTEMPTS TO DELIVER THE MONEY DEMANDED WERE UNSUCCESSFUL. THERE WAS AN ARREST.

1984

NEAR SAN JUAN, PUERTO RICO, TWO POWER PYLONS WERE BOMBED ON 13 SEPTEMBER. ROTATING POWER OUTAGES TO BLOCKS OF 50,000 RATE PAYERS WERE REQUIRED DURING THE TIME IT TOOK TO REPAIR THE PYLONS. DAMAGE WAS PUT AT $100,000.

1984

ON AUGUST 30, A BOMB WAS DISCOVERED ON A GAS SEPARATOR VALVE AT AN OIL PUMPING STATION NEAR FRIENDSWOOD, TEXAS. THE UNKNOWN BOMB LAYER HAD CLOSED A VALVE ON AN INTERMEDIATE PRESSURE GAS SEPARATOR, THEREBY CAUSING A HIGH PRESSURE ALARM TO BE ACTIVATED. THIS ALERTED AN EMPLOYEE WHO DISCOVERED THE BOMB.

1984 - 1985

COMMENCING IN LATE DECEMBER, 1984, AND THROUGHOUT 1985, THERE WERE LABOR DIFFICULTIES AT COAL MINES IN WEST VIRGINIA AND KENTUCKY. THIS UNREST WAS ACCOMPANIED BY A NUMBER OF SIGNIFICANT BOMBINGS, ARSON, BLOCKADES, ASSAULTS, AND HOMICIDE. INSOFAR AS ENERGY SABOTAGE WAS CONCERNED, EVENTS AT OR NEAR THESE COAL MINES DOMINATED 1985. SEVERAL POWERLINES WERE BOMBED, AS WAS AN ELECTRICAL SUBSTATION. COAL MINE EQUIPMENT, SUCH AS SHOVELS, TIPPLES, AND TRUCKS WERE REPEATEDLY BOMBED. SHOOTINGS RESULTED IN ONE DEATH AND SEVERAL WOUNDINGS.

1986

IN A COORDINATED OPERATION ON 14 MAY, UNKNOWN INDIVIDUALS AT THREE LOCATIONS ABOUT THIRTY TO SIXTY MILES FROM THE SITE GROUNDED 500 KV POWERLINES LEADING FROM THE PALO VERDE POWER REACTOR COMPLEX IN ARIZONA. HAD ANY OF THE REACTORS FEEDING THESE POWERLINES BEEN OPERATING - WHICH FOR A VARIETY OF REASONS, NONE WERE - THIS SABOTAGE WOULD HAVE CAUSED THEM TO TRIP. THE COSTS OF SUCH AN OCCURRENCE ARE NOT INCONSEQUENTIAL, AS NOTED PREVIOUSLY.

1987

TWO POWER PYLONS ON A 1,000 KV DC LINE WERE CUT DOWN ON 31 JULY NEAR INDEPENDENCE, CALIFORNIA. THREE OTHER TOWERS WERE DAMAGED WHEN THE CUT TOWERS FELL. AT THE TIME OF THIS SABOTAGE, THE LINE WAS AT LOW VOLTAGE, AND NO POWER OUTAGES OCCURRED AS A RESULT.

1987 - 1988

BETWEEN NOVEMBER, 1987 AND MARCH, 1988, THERE WAS AN INTENSE CAMPAIGN OF SABOTAGE AGAINST ENERGY ASSETS BELONGING TO, OR SUPPLYING COAL MINES IN THE WYOMING - MONTANA BORDER AREA. DAMAGE ESTIMATES FOR THE PERIOD APPROACHED $2 MILLION. ACCORDING TO ACCOUNTS, A DOZEN OR SO POWER POLES - INCLUDING THREE-POLE STRUCTURES - WERE BOMBED; POWER SUBSTATIONS WERE SABOTAGED WITH EXPLOSIVES OR RIFLE-FIRE SEVERAL TIMES; AND RESIDENCES OF OFFICIALS AND COMPANY OFFICES WERE ATTACKED WITH EXPLOSIVES AND INCENDIARY DEVICES. THESE ACTIVITIES CEASED WHEN OWNERS OF THE COAL MINE AND THE UTILITY AFFECTED JOINTLY OFFERED A REWARD OF $250,000 FOR INFORMATION LEADING TO THE ARREST OF ANY PERPETRATOR.

1988

SABOTAGE ACTIVITIES SIMILAR TO THOSE IN WYOMING AND MONTANA WERE DIRECTED AGAINST COAL MINE OPERATORS IN WEST VIRGINIA IN THE PERIOD BETWEEN MAY AND OCTOBER. COAL SCOOPS AND COAL CUTTING MACHINES WERE BOMBED; POWER SUBSTATIONS WERE BOMBED ON AT LEAST SEVEN OCCASIONS; AND SNIPER ATTACKS OCCURRED AGAINST TRUCK DRIVERS AND OTHER PERSONNEL. AVAILABLE DAMAGE ESTIMATES TOTAL ABOUT $750,000.

THE MOST COMMON ACTS OF ENERGY ASSET SABOTAGE OR VANDALISM IN THE U.S. REMAIN THOSE THAT ARE DIRECTED LESS AT ENERGY TARGETS PER SE THAN AT THE INDIVIDUALS WHO OWN OR OPERATE THEM, OR ARE COMMITTED FOR IDLE REASONS. THESE INCLUDE, RESPECTIVELY, GASOLINE STATION BOMBINGS AND ARSON, AND SHOOTING AT POWERLINE INSULATORS OR POWERLINES.

SUBNATIONAL THREATS TO U.S. ENERGY ASSETS

SABOTAGE OF ENERGY ASSETS OUTSIDE THE U.S. - SOMETIMES SPECTACULAR AND OTHER TIMES DEPRESSINGLY PERSISTENT - IT WOULD SEEM HAS CONTRIBUTED TO AN HEIGHTENED INTEREST IN SUBNATIONAL THREATS TO ENERGY SYSTEMS IN THE U.S. ITSELF. THIS IS DESIRABLE, AS IT INEVITABLY HEIGHTENS INTEREST IN ENERGY SYSTEM VULNERABILITIES TO SABOTAGE, WHICH IN TURN LEADS TO EXAMINATIONS OF MATTERS CONCERNING SECURITY, CONSEQUENCE MITIGATION, AND MAINTENANCE OF THE CONTINUITY OF ENERGY SUPPLIES.

THAT BEING SAID, THERE ARE NO INDICATORS OF WHICH I AM AWARE, INSOFAR AS TRENDS IN THE U.S. ARE CONCERNED, THAT WOULD SUGGEST TO ME THE THREAT TO ENERGY ASSETS HERE IS SUBSTANTIALLY DIFFERENT FROM WHAT THE RECENT HISTORICAL RECORD INDICATES. THE PRESENCE IN THE U.S. OF TERRORIST SUPPORT GROUPS DOES NOT ALTER THIS VIEW.

THE SUBNATIONAL THREATS TO ENERGY SYSTEMS IN THE U.S. ARE IN MANY WAYS DIFFERENT FROM THESE THREATS IN NATIONS OTHER THAN THE U.S., INCLUDING THOSE NATIONS WHOSE ENERGY INFRASTRUCTURES HAVE BEEN AND CONTINUE TO BE SUBJECT TO SIGNIFICANT SABOTAGE. THIS IS THE CASE IN INDUSTRIAL AS WELL AS IN PREINDUSTRIAL NATIONS.

THE POSSIBLE RELEVANCE OF THE REALITIES OF SIGNIFICANT TERRORIST SABOTAGE AGAINST ENERGY ASSETS IN EUROPE TO THE THREAT OF SUCH SABOTAGE IN THE U.S. IS WEAK ON A NUMBER OF GROUNDS. PERHAPS THIS CAN BE ILLUSTRATED TO SOME DEGREE BY BRIEFLY NOTING THE CHARACTERISTICS OF THE TERRORIST GROUPS ASSOCIATED WITH SABOTAGE ACTIVITIES THERE.

BELGIUM

THE COMMUNIST COMBATANT CELLS' MOTIVATIONS (INSOFAR AS ENERGY ASSET SABOTAGE HAS BEEN CONCERNED) WERE ANTI-NATO.

FRANCE

ANTI-NUCLEAR POWER AND ANTI-STATISM MOTIVATED THE ASSASSINATION AND PLANNED KIDNAPPING ACTIVITIES OF DIRECT ACTION.

SPAIN

THE MOTIVATION OF ETA FOR ITS LENGTHY CAMPAIGN OF ENERGY ASSET SABOTAGE, INCLUDING ASSASSINATIONS AND KIDNAPPINGS, HAS BEEN SEPARATISM.

WEST GERMANY

THE REVOLUTIONARY CELLS' MOTIVATION, AS THAT OF THE CCC - WITH WHICH THERE MAY HAVE BEEN SOME CONNECTION IN REGARDS ENERGY ASSET SABOTAGE - WAS ANTI-NATO.

THE MOTIVATION OF THE RED ARMY FACTION WAS, AND CONTINUES TO BE, ANTI-STATE. ASSASSINATIONS OF EXECUTIVES ASSOCIATED WITH THE ENERGY SECTOR - IN PARTICULAR, NUCLEAR ENERGY - WERE AN EXPRESSION OF THIS, AS THE RAF CONSIDERS THIS SECTOR TO POSSESS THE CHARACTERISTICS OF STATE AUTHORITARIANISM.

THE RECORD OF ENERGY ASSET SABOTAGE IN THE U.S. DOES NOT REFLECT THE OCCURRENCES OF INCIDENTS MOTIVATED BY THE CONCERNS OF EUROPEAN TERRORISTS. FURTHER, THERE IS NOTHING IN THE U.S. RECORD OF ENERGY ASSET SABOTAGE APPROACHING THE LEVEL OF VIOLENCE, THE INTENSITY OF SABOTAGE CAMPAIGNS, OR THE SOPHISTICATION OF SABOTAGE COMMITTED BY TERRORISTS IN EUROPE.

AT ANOTHER LEVEL IN EUROPE HAVE BEEN THE ACTIVITIES OF THE FEUERABENDTERRORISTEN; MILITANT ELEMENTS OF AN ANTI-TECHNOLOGY MOVEMENT IN THE FEDERAL REPUBLIC. THESE SO-CALLED AFTER-HOURS TERRORISTS WERE MOST ACTIVE IN 1986 AGAINST A BROAD ARRAY OF TECHNOLOGY. THE LEVELS OF ENERGY SABOTAGE WERE UNSOPHISTICATED IN TERMS OF EXECUTION AND RESOURCE UTILIZATION, BUT WERE EFFECTIVE IN SOME INSTANCES. WHAT CHARACTERIZED THIS SABOTAGE AS BEING UNIQUE TO ANY INDUSTRIAL NATION (BEFORE OR SINCE) WAS ITS INTENSITY. SINCE 1986, THE LEVEL OF THIS ACTIVITY HAS DECLINED ABOUT 80 PER CENT. THE FALLOFF OF THIS ANTI-TECHNOLOGY SABOTAGE MAY BE ATTRIBUTABLE TO A NUMBER OF FACTORS, AMONG THEM:

- A LACK OF CONCRETE RESULTS, AND NO FORESEEABLE PROSPECT OF MEETING ANY OF THEIR MAJOR GOALS;
- AN INCREASING SENSE OF ISOLATION DUE TO FAILURE TO JUSTIFY TO ANY SIGNIFICANT ELEMENT OF THE GENERAL POPULATION THEIR MEANS TO THE END;
- STRESS FROM CONCERNS ABOUT POTENTIALS FOR INJURIES OR ARRESTS;
- ARRESTS;
- AGEING OF THE CADRE AND INSUFFICIENT RECRUITMENT OF YOUNGER INDIVIDUALS; AND,
- INCREASING SECURITY AT FAVORED TARGETS.

IN ANY EVENT, WHILE THE TYPES OF SABOTAGE COMMITTED BY THESE AFTER-HOURS TERRORISTS MAY MIMIC TO SOME DEGREE INDIVIDUAL ACTS COMMITTED IN THE U.S., WIDESPREAD MILITANT ANTI-TECHNOLOGY MOTIVATION IS NOT A FACTOR HERE.

SABOTAGE THREATS TO ENERGY ASSETS IN PREINDUSTRIAL NATIONS ARE IN GENERAL MORE SEVERE THAN IN INDUSTRIAL NATIONS FOR A NUMBER OF REASONS. THESE INCLUDE SYSTEM AND ENVIRONMENTAL CONSIDERATIONS.

WITH REGARD TO SYSTEMS: THEY OFTEN LACK REDUNDANCY, DUE EITHER TO TERRAIN OR TO THE WAYS IN WHICH THEY WERE ORIGINALLY BUILT. FOR EITHER REASON, INTERCONNECTING GRIDS - IN THE CASE OF ELECTRICAL DISTRIBUTION SYSTEMS - MAY BE INADEQUATE TO COPE WITH SABOTAGE TO ALMOST ANY ELEMENT OF THE SYSTEM. THIS SITUATION SOMETIMES PERTAINS IN FORMER COLONIES WHERE ELECTRICAL DISTRIBUTION SYSTEMS FOLLOW ROADS ORIGINALLY BUILT BY THE COLONIZING POWER. THESE ROADS FOR THE MOST PART WERE NOT BUILT TO PROVIDE TRANSPORTATION SERVICES TO THE INDIGENOUS POPULATION, BUT TO FACILITATE THE REMOVAL OF ORE, TIMBER, OR OTHER GOODS TO THE COAST. IN MANY SUCH SITUATIONS, THE ROADS DID NOT FORM NETWORKS, AS THEY WERE NOT INTERCONNECTED. THE SAME PERTAINS WITH THE ELECTRICAL SYSTEMS, BUILT MUCH LATER, AS THESE FOLLOWED THE EXISTING ISOLATED ROADS.

THIS, IN PART, IS THE REASON INSURGENT GROUPS IN SUCH PLACES AS SURINAME AND MOZAMBIQUE CAN, WITH THE EXPENDITURE OF THE MOST MEAGER RESOURCES, HAVE SUCH DISPROPORTIONATE EFFECTS ON THE ECONOMIES OF THESE NATIONS.

FOR A SIMILAR EXPENDITURE, INSURGENTS IN COLOMBIA HAVE VIRTUALLY HELD HOSTAGE THAT COUNTRY'S PATRIMONY, AS REPRESENTED BY THE VALUE OF CRUDE OIL IN THE GROUND, BY REPEATEDLY BOMBING THE PRINCIPAL PIPELINE THROUGH WHICH THE LIFTED CRUDE IS TRANSPORTED. HERE, TARGET ISOLATION OPERATES TO EASE THE TASK OF THE INSURGENT, AS DOES THE ABILITY OF THE INSURGENT TO DENY ACCESS TO THE AREAS OF SABOTAGE, IF ONLY TEMPORARILY.

PERHAPS NOWHERE IN THE WORLD HAVE THE FACTORS OF ISOLATION AND AREA DENIAL CAPABILITY BEEN MORE EXPLOITED THAN IN THE CAMPAIGN OF ELECTRICAL SYSTEM SABOTAGE IN EL SALVADOR, WHERE THE INTENSITY OF THIS ACTIVITY IS NOWHERE EXCEEDED.

IN THE ANDEAN NATIONS, TERRAIN IS THE INSURGENT'S ALLY. THE ANDES FORM NATURAL BARRIERS THAT, FOR THE MOST PART, HAVE NOT BEEN TRAVERSED BY POWER SYSTEMS EXCEPT THROUGH A FEW BISECTING VALLEYS, THROUGH WHICH TRAILS WERE ESTABLISHED IN THE 16th AND 17th CENTURIES: PRESENT DAY ROADS USUALLY FOLLOW THE ORIGINAL TRAILS. THE TERRAIN IS DIFFICULT. SABOTAGE CAN OFTEN TAKE DAYS TO REPAIR, IN PART DUE TO TERRAIN DIFFICULTIES. INSURGENTS HAVE TAKEN ADVANTAGE OF THE EXISTING SITUATION, AND WITH MODEST RESOURCES APPLIED IN RUDIMENTARY FASHION, CAN PRODUCE EFFECTS FAR BEYOND WHAT WOULD BE POSSIBLE IN DIFFERENT CIRCUMSTANCES.

VERY LITTLE OF WHAT GOES ON WITH REGARD TO ENERGY SABOTAGE IN PREINDUSTRIAL NATIONS IS COMPARABLE TO WHAT OCCURS IN THE U.S. EXCEPT, PERHAPS, THE FACT THAT THE SABOTAGE ITSELF IS RELATIVELY UNSOPHISTICATED. WHAT PARALLELS MAY BE FOUND BETWEEN THE RECORDS OF ENERGY ASSET SABOTAGE IN PREINDUSTRIAL NATIONS AND IN THE U.S. REINFORCE MY PERSPECTIVE CONCERNING TRENDS IN THE U.S. WHICH IS TO SAY THAT THERE APPEAR TO BE NO INDICATIONS THAT SUCH TRENDS WILL DIVERGE IN ANY SIGNIFICANT WAY FROM WHAT THE HISTORICAL RECORD SUGGESTS.

ENERGY ASSETS AFFECTED IN SUBNATIONAL INCIDENTS - 1980 through Dec 1988

Target Summary

Target Type	Number Affected
Power pylons/ power lines	7,290
Fuel tanker trucks	1,844
Power substations	436
Petroleum/gas pipelines	343
Petroleum storage tanks/storage depot	339
Central power stations	334
Personnel	303
Service stations	238
Corporate/government offices	154
Truck/car	91
Support facilities	80
RR tank car	78
Refinery	67
Mine	51
Oilwell/field/camp	47
Local power generator	46
Railroad	45
Construction site	29
Construction equipment	20
Helicopter/fixed wing aircraft	16
Pipeline pumping station	16
Industrial power plant	15
Deep sea vessel/lighter	13
NG/LPG 'facility'	12
Spent nuclear fuel	8
Barge	7
Nuclear waste	7
Train	3
Offshore platform	1
TOTAL	11,933

SUBNATIONAL INCIDENTS AFFECTING ENERGY ASSETS - 1980 through Dec 1988

Data Base Summary

	1980	1981	1982	1983	1984	1985	1986	1987	1988	Total
Afghanistan	3		7	22	37	38	6	18	22	153
Angola	1	1		3	26	17	12	4	28	92
Antigua & Barbuda									2	2
Argentina					1		1	4	2	8
Australia	1			2			1			4
Austria					1		3			4
Bahrain								1		1
Bangladesh							1	5		6
Belgium	1				4	5				10
Bolivia		8		1	2	1	1	1	2	16
Brazil				1			2	2	3	8
Burma				1					10	11
Canada	7	1	4				1		2	15
Chad						1				1
Chile	1	6	6	21	107	32	46	32	57	308
China (PRC)		1							5	6
Colombia	3	18	3	4	6	22	47	36	111	250
Congo	1									1
Corsica					1				2	3
Costa Rica				2	1	1				4
Cyprus						1				1
Czechoslovakia							1	1		2
Denmark			1				17	19		37
Djibouti									2	2

	1980	1981	1982	1983	1984	1985	1986	1987	1988	Total
Dominica		1								1
Dominican Republic								2		2
Ecuador				1	3		1	1		6
Egypt		2								2
El Salvador	21	140	91	88	112	111	37	39	141	780
Eritrea					1		3			4
Ethiopia						1		2	5	8
Fiji								1		1
France	20	9	11	3	5	10	7	3	2	70
Greece	2		1			1	4		2	10
Guatemala	1	15	30	1	2	9	5		6	69
Guinea									1	1
Haiti							1	3		4
Honduras	1	1	5	1					3	11
Hong Kong		1								1
India	3	3			3	2	3	14	4	32
Indonesia		1								1
Iran	24	5	2			3	1	7		42
Iraq	2		2		1	8	21	31	9	74
Ireland		1	1							2
Israel	3	2				1	3	2	4	15
Italy	5	1		1		1	2	7	6	23
Jamaica		2								2
Japan	1	4	2		1	1	2	1	9	21
Jordan						1				1
Kampuchea				1	19	4	18	11	4	57
Kenya			1							1

	1980	1981	1982	1983	1984	1985	1986	1987	1988	Total
Kuwait		2		2			1	4		9
Laos									1	1
Lebanon		2	8	1	1		3	1		16
Lesotho				2	1					3
Libya		1						1		2
Luxembourg						6				6
Malaysia							2			2
Maldives									1	1
Mexico		2			1	1	1		4	9
Morocco					1					1
Mozambique	3	6	9	7	15	12	9	23	23	107
Namibia	1	1	1	2	3	1	5	3	2	19
Netherlands	2	1				3	6	1	6	19
New Caledonia						1	1		2	4
Nicaragua		1	2	15	9	9	3	34	11	84
Niger			1	1						2
Nigeria								2	2	4
Northern Ireland								3		3
Norway		1	1							2
Pakistan				4		2	6	5	9	26
Palestine								2	2	4
Panama				1		1		1	1	4
Papua New Guinea									2	2
Peru	2	18	35	25	21	45	49	40	49	284
Philippines		2			6	13	10	16	8	55
Poland		3					1		1	5
Portugal						2				2
Saudi Arabia								1	3	4

	1980	1981	1982	1983	1984	1985	1986	1987	1988	Total
Senegal									1	1
Sierra Leone								3		3
Singapore								1		1
Somalia		1			4	4	1	2	2	14
South Africa	3	7	7	5	9	29	27	6	4	97
South Korea									1	1
South Yemen			2				2			4
Spain	13	34	9	2	2	1	1	3	13	78
Sri Lanka			1		1	4	5	4	22	37
Sudan		1		2	2	3	3	4	2	17
Suriname				2	2		4	8		16
Syria		1	1	1		1				4
Switzerland	3	3		3	1					10
Taiwan									2	2
Thailand		1							1	2
Trinidad & Tobago	1					1				2
Tunisia					1					1
Turkey	6	1	2	2	2		8	10	2	33
Uganda		1			3	1				5
USSR							1		5	6
UAE						1				1
United Kingdom	6	1			3	1	1	2	3	17
UNITED STATES	44	43	32	29	19	27	25	27	38	283
Uruguay								1		1
West Germany	4	4	5	1	6	29	153	7	18	227
Western Sahara					1	2				3
Yugoslavia							4	3		7

	1980	1981	1982	1983	1984	1985	1986	1987	1988	Total
Zaire						1				1
Zambia							1			1
Zimbabwe		1		2						3
TOTALS	188	362	283	262	447	472	582	464	685	3,745

*In many instances, the numbers of incidents are understated. Some accounts are summaries of multiple incidents in which the separate incidents are not listed.

Testimony of
Randall W. Hardy, Superintendent
Seattle City Light

Before the
United States Senate
Committee on Governmental Affairs

February 8, 1989

Mr. Chairman and Members of the Committee: My name is Randall W. Hardy. I am Superintendent of Seattle City Light, the nation's seventh largest municipally-owned electric utility. I have held this position for the past four years; prior to that, I have served as the Executive Director of the Pacific Northwest Utilities Conference Committee, as Puget Sound Area Manager for the Bonneville Power Administration, and as Executive Assistant to the Administrator of the old Federal Energy Administration.

Today I am pleased to provide you a description of the effects of a significant electrical outage in an urban environment, based on the recent experience of Seattle City Light.

At 11:02 a.m. on Wednesday, August 31, 1988, an intense fire in an underground electrical vault caused extensive damage to six 13,000-volt feeder cables, two 500-KVA network transformers and numerous lower voltage cables. The relaying out of the six 13,000-volt feeders cut power to approximately 50 square blocks of Seattle's downtown business district; roughly one-third of the downtown underground electrical grid. Power was not restored until 6:47 p.m. on Saturday, September 3, 1988, ending the worst blackout in City history.

At the height of the four day blackout, nearly all of the hundreds of businesses in the affected area were closed. The loss of lighting, air conditioning, computer, security, fire detection, refrigeration, telephone and elevator systems virtually mandated that such was the case. Businesses impacted included approximately 130 restaurants, 55 shops, a major department store and several motion picture theaters. Many popular nightclubs closed and several hotels had to shift guests to other establishments outside of the outage area. Numerous food service establishments gave away their inventory before it spoiled, and thousands of workers experienced extra time off as part of their Labor Day weekend. The financial loss to these businesses has been estimated to be in the hundreds of thousands of dollars and may reach into the millions.

The thousands of citizens who resided in the affected area were severely impacted. Their lights and electrical appliances were unavailable to them, and as Seattle was experiencing unusually hot temperatures in the high 90's, the loss of air conditioning was onerous. A particular population at risk were the elderly and low-income residing in the area of the outage. Hundreds who live in high-rise buildings were either stranded in their upper apartments without electricity and water or forced to take up temporary residence in first floor lobbies as elevators were unable to return them to their residences.

On the streets, the lack of traffic signals and streetlights, coupled with the absence of security and fire alarm systems, raised considerable concern over the safety of the public and property. While the use of virtually every portable electric generator in the western half of the State of Washington provided support to some residents and businesses, at night the outage area was dark and exposed. Fortunately, as a result of the rapid isolation of the outage area, saturation patrols by police and fire personnel, the prompt rigging of temporary streetlighting, and probably most critical of all, the good will and cooperation of the people of Seattle, there were no significant incidents of civil disruption, theft or property damage.

This avoidance of dire consequences, I believe, was the fortunate theme of our experience. Indeed, I would suggest that you consider our event as a best-case rather then a worse-case experience. Given our cause - a loss of power to one-third of our downtown business area for four days - our effects were probably as minimal as one could hope for. There were moments of concern, when individuals were trapped in elevators or window-washing rigs. There was considerable discomfort and inconvenience for tens of thousands of citizens during the outage and in its immediate aftermath. There was sustained and exemplary work by hundreds of City and social agency employees. There were substantial business losses and costs to City Departments of hundreds of thousands of dollars. Nevertheless, there were no fatalities, no serious injuries, no significant traffic accidents, and no major property damage as a result of this event. This, in retrospect, is miraculous, and should not be expected in any recurrence of such an outage.

Many factors point to this conclusion. First, the vault fire did not involve the rupturing of the transformers, which would have produced considerable damage and risk, either through the immediate explosion that would occur or the release of potentially PCB-laden smoke.

Second, the timing of our outage was nearly ideal, as it occurred in the midst of hot, dry summer weather, on days extending into the three-day Labor Day weekend. This served to minimize the effect, to some degree, on all the populations involved.

Third, the response of the citizenry of the City of Seattle was superb. A spirit of cooperation and support was evident throughout, and the potential of crime or civil disorder never manifested itself.

Fourth, the efforts and coordination of the agencies responding were of the highest level. Employees of several City of Seattle Departments - Light, Fire, Police, Engineering, Health - worked long and hard to maintain a framework of basic services and to restore power. Social agencies, particularly the Red Cross, provided extraordinary support to the citizens and workers within the outage area.

Finally, the size and duration of the outage, while major, remained manageable. City Departments and social agencies were able to respond by the redeployment of existing staff and resources. However, by the end of the outage these had been extended to the point that they were rapidly wearing down. In my judgement, had the outage hit an area twice as large, most impacts would have increased exponentially rather than linearly.

I would now like to describe for you several of the lessons learned as a result of this event which I believe are pertinent to any discussion of addressing urban disasters.

First, effective management of the response team is the critical variable of the equation. It was essential to quickly establish a single point of leadership, the role of which is to provide policy direction, resolve disputes among work units, remove obstacles impairing work progress and provide leadership visibility to the workforce and the general public. In terms of managing the workforce, such direct leadership was necessary to establish centralized policy direction while at the same time allowing decentralized implementation of those policies. Seattle City Light established a routine in which all the key players within the Department met early each day to review our current status, chart our course for the next 24 hours, and make the required policy and non-technical decisions. Subsequent to these meetings, individual managers, supervisors and crew chiefs at a variety of work locations made the technical decisions necessary to advance the restoration of power. For an event of this magnitude, daily meetings were sufficient to put everyone on the same base and accomplish the necessary coordination without becoming a hindrance to production. At the crew level, it was found to be particularly valuable to maintain a cumulative log of events as crews went on and off duty on their 12-hour shifts, to brief incoming crews somewhere other than their work site, and to overlap crew rotations for one hour to ensure an uninterrupted assault on the problem at hand. Each of these practices served to facilitate our efforts to replace 3,000 feet of high voltage underground cable, 6,000 feet of service voltage underground cable, and to provide switching services at over 100 locations.

A second lesson learned is the requirement to establish early and solid coordination with all other agencies involved in the response. As I stated earlier, good coordination and cooperation were key in our efforts. In addition to our separate responsibilities, Seattle City Light worked with the Red Cross in providing services to special need populations, with the Police Department in providing temporary streetlights, with the Fire Department in providing and hooking up emergency generators, with the Engineering Department in reestablishing traffic control systems and the Health Department for the closure of restaurants.

A third lesson learned was the necessity of developing and utilizing emergency operations plans. While existing emergency management plans did not perfectly "fit" the event we experienced, they did establish the framework for our response and served to enhance our efforts.

A fourth lesson is the invaluable contribution of communications technology. The use of mobile phones was critical. These devices allowed continuous one-to-one communication, while more traditional radio communications were utilized for multi-party information distribution. The availability of mobile phone technology upgraded our ability to respond and must be part of any emergency management process, as the need for rapid and extensive communication is paramount.

A final lesson I would stress is that of media coordination. The media was invaluable in spreading information regarding the outage and in controlling its effects. In dealing with over 500 media contacts during this brief period, it was essential that a knowledgeable source provide clear messages, at designated places and times. I found it valuable to present messages live, from the outage site, during the morning, mid-day and evening news slots. It was critical to have a designated public information person available at this location at all hours and to have them possess the critical information that the public needed. By being able to provide consistent information, the image of competence and control is established and maintained, the technical experts working in the field are separated from the distractions of the media, and the public is kept informed.

In summary, while our experience was significant, its consequences could have been much more dire, and they probably will be if there is a next time. Nationwide, there will undoubtedly be next times, whether the result of natural disaster, infrastructure failure, or an act of terrorism. Our dependency on electricity is ever-increasing but seldom noted. Prudent actions to minimize the occurrence of electrical power system failures as well as to control their effects have never been more advisable and necessary.

I thank the Committee for this opportunity to discuss the experience of Seattle City Light and would be pleased to respond to any questions.

BW:cb(T)

STATEMENT OF CHARLES H. WHITE
NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION
BEFORE THE
U.S. SENATE GOVERNMENT AFFAIRS COMMITTEE
FEBRUARY 7-8, 1989

SUBJECT: THE CURRENT AND PROJECTED CAPABILITIES OF INDUSTRY TO RESPOND TO A POTENTIAL CRISIS, AND HOW PRESENT INVENTORY AND MANUFACTURING POLICIES POTENTIALLY AFFECT RECOVERY EFFORTS

Mr. Chairman:

I am Charles H. White of the National Electrical Manufacturers Association (NEMA). I want to thank you for this opportunity to present the concerns of NEMA and its members on the capability of the U.S. heavy electrical equipment manufacturing industry and related capability to assist electric utilities in recovering from severe and widespread damage to U. S. electrical systems, 242kV and greater.

NEMA is the principal national trade association of the electrical manufacturing industry; the Association has over 600 member companies manufacturing electrical products in the U.S. that are used either as components of, or as end-equipment in all major phases which generate, transmit, control, and utilize electricity.

Comments on capability and policy will apply to all of the major capital components used in such systems; but, for the purpose of illustration, I will focus on large power transformers. This is because that sector has been most thoroughly studied and has the largest data base for comparison purposes. Today, in my examples, I will be referring to the 40MVa and up transformer product classification. These transformers perform the key function of stepping up voltage from the generating plant for transmission and stepping down the voltage for use in the distribution system. (See attached electric system schematic.) These are extremely large pieces of equipment (see attached picture), made to the specific requirements of the purchasing utility. Because of their size, large manufacturing facilities, overhead cranes, and specialized manufacturing installations are required for their construction. Also required is equally large test apparatus and facilities. Under optimum conditions, it takes about one year to manufacture one of these large transformers. What happens to large power transformers is representative of the entire heavy electrical equipment industry.

Before going into detail, I will summarize the type of equipment of concern, as well as comment on energy demand. Thereafter, I will comment on the current and projected capabilities of the manufacturers to respond to a potential crises, such as massive damage or destruction to a percentage of the existing capital plant of the electrical utility industry, and how present inventory and manufacturing policies affect recovery efforts.

We are not talking about distribution equipment, (that is the gray equipment most often seen on poles or enclosed in green padmounted cabinets in residential neighborhoods) nor is it the equipment seen in small utility parks known as distribution substations.

NEMA's testimony today, Mr. Chairman, concerns heavy electrical equipment located at electric power generating plant switch yards, electric utility power system switching centers, etc.

Since the early 1980's, annual energy forecasts have reduced the expected total demand for energy annually through the year 2000. In fact, total demand for energy has declined as a result of conservation, improved product design, energy efficient processes, etc. However, the growth in electric energy demand has remained relatively constant at its long term historical (100 year) growth rate of 2.0%-3.0% per year. Thus, we are less dependent on certain energy sources; but more dependent on electrical energy to maintain our economic and material standard of living.

Mr. Chairman, the current and projected capabilities of the heavy electrical equipment manufacturing industry have been significantly changed by restructuring within the industry. In the large power transformer sector alone, nearly 40% of the U.S. production capacity has been removed in the last 30 months. This is due to utilities reaching the end of capital investment cycles which, combined with a slowing in the 7% yearly increase in electric energy demand of the late '60s & early '70s, has resulted in a decrease in demand for equipment used in electrical systems.

Thus, the reduction in the manufacturing capacity for heavy electrical equipment is a rational response to a down-sized domestic market for such equipment. However, it should also be noted that the reduction in domestic electrical equipment manufacturing capacity is also impacted by a world wide surplus of such capacity, the causes of which are only partly analogous to the U.S. situation.

The problem is that today's domestic manufacturing industry is expected to support a utility capital plant base constructed, installed, and maintained on a manufacturing capacity which was 100% larger just three years ago.

Given the current utility capital plant base, any act which damaged as little as 10% of that plant would result in demand for billions of dollars of goods. For example, we assume 3,000 large power transformers manufactured since 1968 = 300 transformers requiring either repair or replacement. Total annual U.S. production rate is approximately 100 large power transformers. Utility capital plant recovery time might be as short as three years (assuming only 150 new transformers need to be produced and pushing production up 50%, or as long as 6 years (assuming a total of 300 new transformers need to be produced and pushing production up 50%).

THE BOTTOM LINE: Without a meaningful commitment, by both utilities and government, to maintain a domestic manufacturing capability to support some identified surge in demand for capital equipment, U.S. manufacturing capability will continue to decline, becoming less able to respond to a crisis as time goes on.

In related discussions of Inventory and manufacturing policies, one might be tempted to seek a solution by purchasing and storing needed equipment. However, such an approach overlooks the customized nature of heavy electrical equipment. Specifically, the design criteria and the application requirements for each such piece of capital equipment are so unique that it would be necessary to maintain a substantial number of individual replacement items. NEMA feels that the most effective way to inventory products is to have the manufacturing assets needed in an emergency. This approach has the added benefit of maintaining industrial viability and ensuring continued access to improved technology in product design, manufacture, and application.

Manufacturers have no incentive to retain large and expensive manufacturing assets, large highly capitalized engineering teams for product design, as well as manufacture and finally, the large and highly skilled cadres of craftsmen necessary to actually build products. Consequently, manufacturers today are continuing to reduce production capacity: First, by reducing the size and depth of engineering and manufacturing teams; Second, by focusing on specific technologies within product sectors in order to achieve commercial advantage in a market.

What should be noted is that in spite of continuing erosion in the electrical manufacturing industry, the U.S. is the world leader in heavy electrical equipment manufacturing, both in technology and economic efficiency.

To a degree, the situation may be different in the near future because of economic circumstances and political decisions and, to a greater degree, because of unrestrained, unfair foreign competition in the U.S. as well as in world electric equipment markets.

Foreign manufacturers of heavy electrical equipment have, consistently over time, been able to sell their products in the U.S., while their home markets have been effectively closed to U.S. manufacturers. In many cases, institutionalized protection has provided a substantial subsidy, enabling foreign companies to undercut U.S. goods in both the American market, as well as third country markets. Such competition displaces U.S. producers and forecloses future commercial opportunities (see attachments). Since 1971, the number of jobs in the heavy electrical equipment industry, just for the manufacture of large power transformers, has fallen from 10,000 to less than 4,000. The dilemma today is that, once the investment in facilities, resources and personnel are redirected, our ability to refocus assets and resources under disaster conditions remains to be demonstrated. This situation has been identified and reported by NEMA for some time. In fact, NEMA has long argued for Fair Trade consideration in the U.S. approach to trade policy, tax policy, regulation, etc.

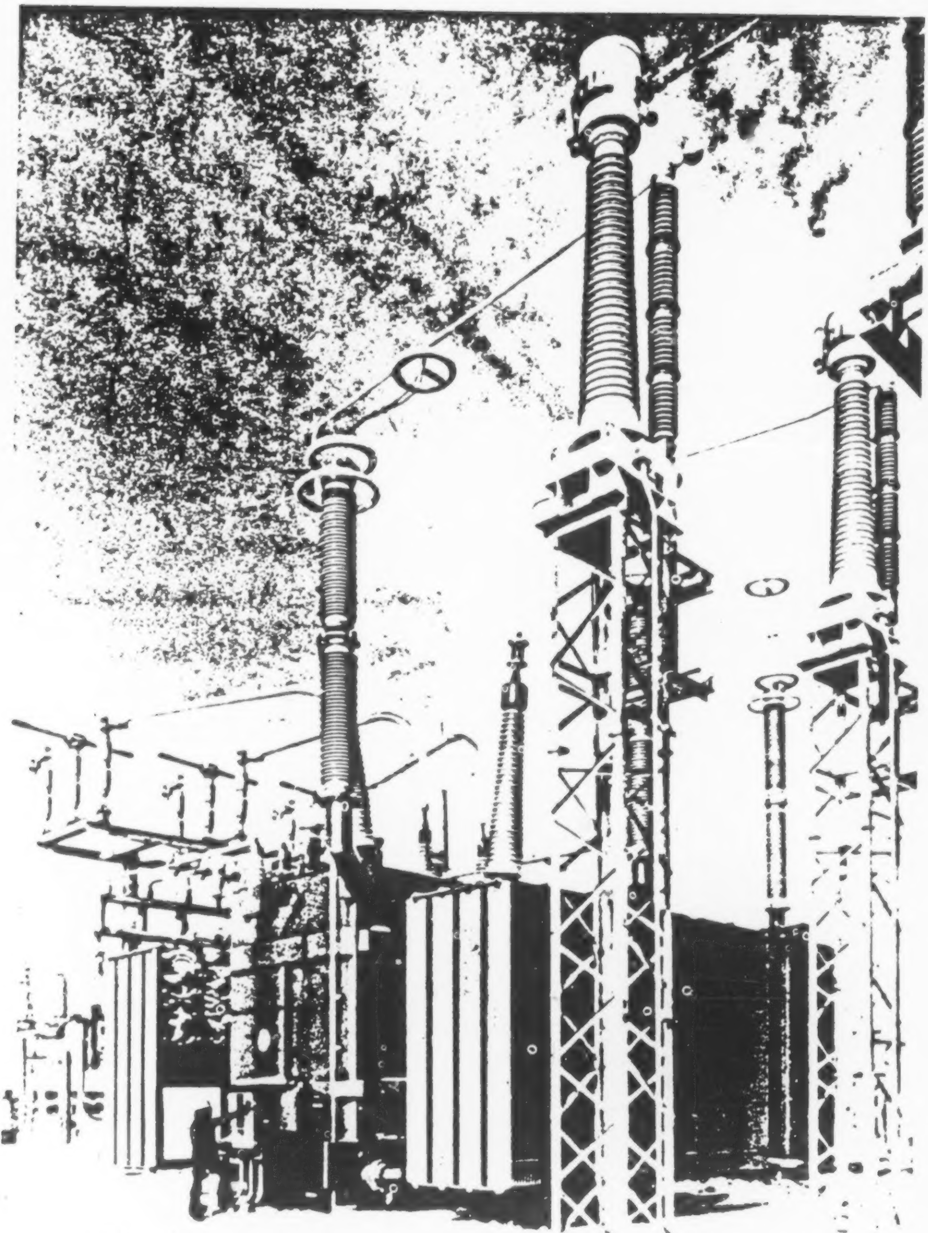
Attached to my statement are copies and excerpts from previous testimony to selected committees of Congress and federal agencies. These excerpts are provided to explain in greater detail how foreign procurement policy and trade practices have affected the U.S. manufacturing industry.

Without viable markets, or the expectation of such markets, U.S. electrical equipment manufacturers cannot make the investments necessary for a domestic electrical equipment manufacturing capability. In some instances, reduced production capacity will be partially offset by foreign manufacturers purchasing assets and then changing production activity from manufacture to assembly; conducting design, R&D, and manufacturing key components in their home country.

The question for us is a simple one. Does the United States desire to retain a domestic heavy electrical equipment manufacturing industry? Our trading partners have had occasion to address this question relative to their own industries. We know their answer - concerted efforts by the U.S. Government to reduce the propensity of our trading partners from favoring their own domestic manufacturers have met with little success. This is due largely to their interest in retaining a domestic manufacturing capacity for security reasons.

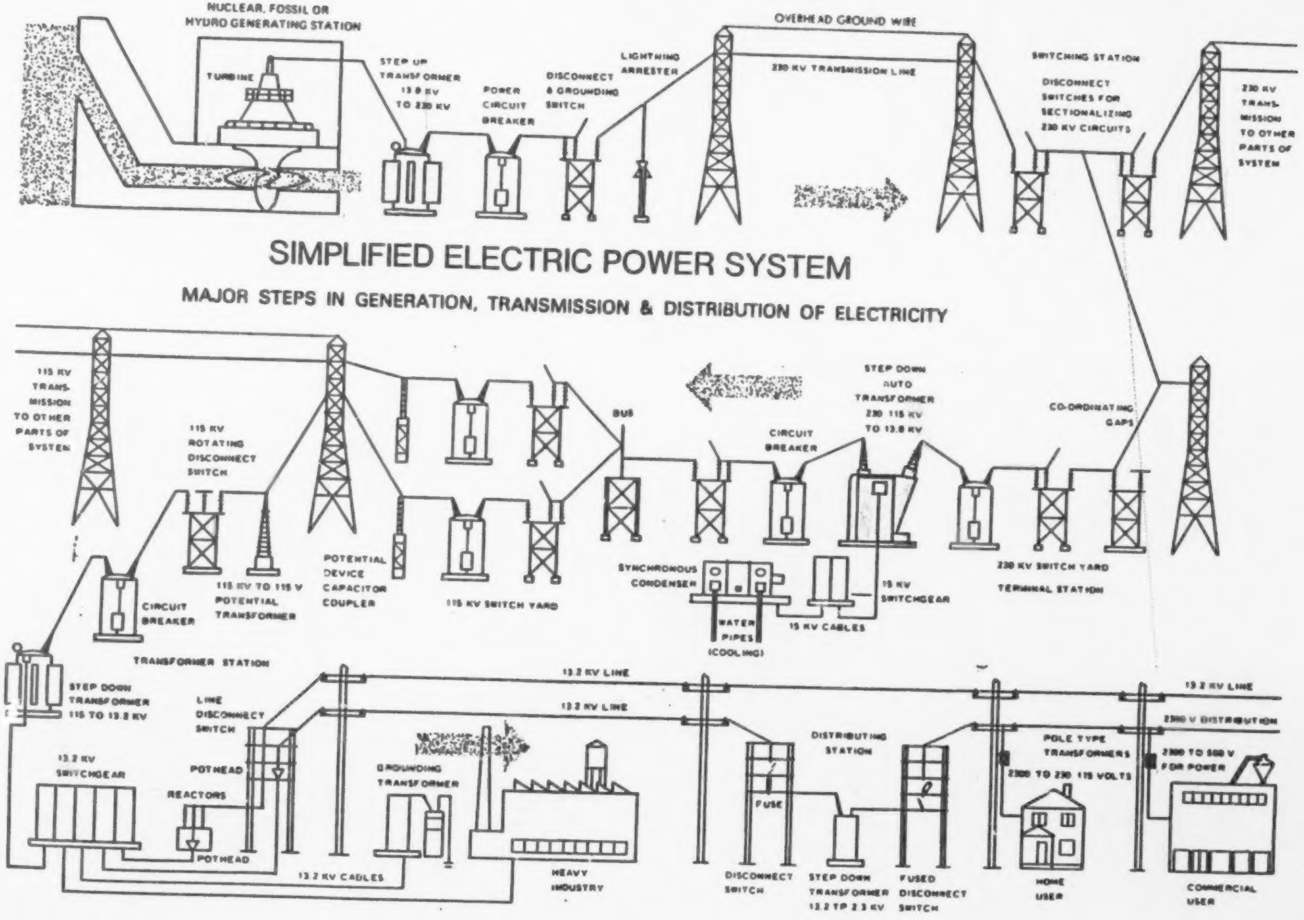
The manufacturers stand ready to assist you in any way, as you continue your investigation of this issue.

Thank you, Mr. Chairman.



SIMPLIFIED ELECTRIC POWER SYSTEM

MAJOR STEPS IN GENERATION, TRANSMISSION & DISTRIBUTION OF ELECTRICITY


NUCLEAR, FOSSIL OR HYDRO GENERATING STATION
TURBINE
STEP UP TRANSFORMER 13.8 KV TO 230 KV
POWER CIRCUIT BREAKER
DISCONNECT & GROUNDING SWITCH
LIGHTNING ARRESTER
OVERHEAD GROUND WIRE
230 KV TRANSMISSION LINE
SWITCHING STATION
DISCONNECT SWITCHES FOR SECTIONALIZING 230 KV CIRCUITS
230 KV TRANS-MISSION TO OTHER PARTS OF SYSTEM
115 KV TRANS-MISSION TO OTHER PARTS OF SYSTEM
115 KV ROTATING DISCONNECT SWITCH
CIRCUIT BREAKER
115 KV TO 115 V POTENTIAL TRANSFORMER
POTENTIAL DEVICE CAPACITOR COUPLER
115 KV SWITCH YARD
BUS
CIRCUIT BREAKER
STEP DOWN AUTO TRANSFORMER 230 115 KV TO 13.8 KV
CO-ORDINATING GAPS
SYNCHRONOUS CONDENSER
WATER PIPES (COOLING)
15 KV CABLES
15 KV SWITCHGEAR
230 KV SWITCH YARD
TERMINAL STATION
TRANSFORMER STATION
STEP DOWN TRANSFORMER 115 TO 13.2 KV
LINE DISCONNECT SWITCH
13.2 KV SWITCHGEAR
POTHEAD
REACTORS
POTHEAD
13.2 KV LINE
13.2 KV LINE
GROUNDING TRANSFORMER
13.2 KV CABLES
HEAVY INDUSTRY
DISTRIBUTING STATION
FUSE
DISCONNECT SWITCH
STEP DOWN TRANSFORMER 13.2 TP 2.3 KV
FUSED DISCONNECT SWITCH
13.2 KV LINE
2300 V DISTRIBUTION
POLE TYPE TRANSFORMERS
2300 TO 230 115 VOLTS
2300 TO 550 V FOR POWER
HOME USER
COMMERCIAL USER

STATEMENT OF CLAUDE E. HOBBS
BEFORE
THE INTERNATIONAL TRADE COMMISSION
WASHINGTON, D. C.
SEPTEMBER 28, 1982

I am Claude Hobbs, Vice President-Senior Counselor of Westinghouse Electric Corporation. I am here today to testify on behalf of the National Electrical Manufacturers Association (NEMA).

NEMA is the principal national trade association of the electrical manufacturing industry. The Association has some 550 member companies manufacturing electrical products that are used either as components or as end-equipment in all major phases which generate, transmit, control and utilize electricity. Of prominent note are large steam turbine generators, large power transformers, and high voltage power circuit breakers. They are major products required by electric utilities to generate electricity and transmit it to population centers for use.

Working through NEMA, the electrical equipment industry on several occasions has undertaken to prepare reports on the economic impact of business lost by virtue of international trade discrimination. U.S. Government statistics, unfortunately, are meager and inadequate, and we have found it anything but easy to get relevant information from the member companies of this organization. Accounting data maintained for industrial and commercial purposes are often not readily adaptable for use in specialized economic impact studies. Obtaining information of this type is even more difficult because the large electrical equipment industry is composed of only a small number of competing companies. NEMA and its members, therefore, particularly welcome this study by the ITC.

There is much comment nowadays that we are witnessing the development of a worldwide, international industrial marketplace. Many economists have expressed a feeling that the United States is losing position in this world marketplace at a time when competition between nations to achieve and maintain an important position is already keen and is becoming more aggressive.

The governments of other industrialized countries place great emphasis on the export of industrial products. They assist their manufacturers in many ways with their government industrial policies, and one powerful form of such assistance is export financing.

Large and very expensive plants and equipment are needed to manufacture electrical machinery of the magnitude and sophistication required to generate and transmit electricity. Equally important, if not more so, are the large numbers of specialized engineers and highly skilled experienced workers who produce the machinery.

A flow of orders is necessary to maintain these skilled people as ready teams, and to have available the very expensive manufacturing facilities when they are needed to produce the large equipment required by electric utilities in the United States and in other countries.

Conversely, a loss of orders because of foreign government export financing, whether for U.S. domestic use or for export, causes distress to personnel and the expense of idle plant capacity.

Prior to 1973, electric energy consumption in the United States was growing at 7 or 8% each year. The use of electricity was also growing in other areas of the world, notably in the less developed countries which are industrializing and improving their standards of living.

Since the OPEC oil boycott, the growth of electrical use in the United States has been curtailed sharply as a result of slowdown in industrial expansion, conservation, and recently because of extremely high interest rates. New orders from American utilities for large electrical equipment have fallen off sharply, and many previously existing orders have been cancelled or their delivery postponed.

Although the volume of orders has fallen in the United States, foreign business is available for American producers, but only from the developing nations. Japan and European countries which are capable of making the large equipment under discussion have long had rigid policies and practices which effectively boycott the purchase of American-made electrical equipment.

While American manufacturers confront a much reduced domestic market for large electrical equipment, aggressive competition in our home market from Europe and Japan continues at prices which are usually much lower than foreign home market prices. In addition to very low prices, American manufacturers have now encountered an offer of low-cost foreign financing for sale of foreign-made equipment to a United States electric utility company. We are apprehensive that this is just the beginning of foreign governments' assistance to their manufacturers to penetrate the American market. Foreign competition, except for a modest import duty and a small Buy-American Act differential for Government purchases, is not restricted in the United States. Yet our members are practically shut out of the markets of Europe and Japan, and when they endeavor to sell to third world countries, they face foreign competition which is usually supported by foreign government export financing at below market rates.

As already stated, the developing countries are today's main potential markets for United States large electrical equipment export business. American manufacturers are anxious and able to compete in those markets with other manufacturers. When the competition is limited to price, delivery, and quality, our members can be successful. But when competition includes factors over which they have no control, that is, foreign government cut-rate export financing, the ability of United States companies to compete is greatly diminished.

We cannot emphasize too strongly that the economic impact of business lost by American electrical equipment manufacturers is much the same, whether the lost orders were for equipment to be used in the United States or in foreign countries. It is the cumulative impact of all lost business that severely affects the cost of idle plant capacity and the distress of unemployed personnel. Lack of orders also deprives American manufacturers of income essential to support research and development, without which we lose our competitive technological edge.

American electrical equipment manufacturers have no fear of being able to hold their own in free and fair competition with Japanese and European manufacturers, but such competition does not exist. Confronted with the financing practices of the governments of Japan and Europe, American exporters are having to compete in a war they alone can't win.

One billion dollars of production of electrical equipment in the United States supports at least 24,000 man-years of employment in the United States - the Department of Commerce previously estimated up to 30,800 man-years. This employment provides economic benefit in the form of state and local taxes, and obviates the burdens of unemployment compensation and other social assistance. In addition, there is the economic multiplier effect generated when each worker spends his income for food, housing, clothing, transportation, insurance and recreation.

Wharton Econometric Forecasting Associates have done a study of the economic impact of a proposed Export-Import Bank loan to support the sale of mass transit equipment to Argentina. The study concluded that such a loan would result in a nine-to-one benefit to the United States. While this and another Wharton study were conducted for a different purpose than the study now being made by the International Trade Commission, the Wharton conclusions concerning economic benefit from orders received by U.S. manufacturers should be of interest to the Commission in connection with an analysis of orders lost owing to foreign government export financing.

National Electrical Manufacturers Association

STATEMENT OF

BERNARD H. FALK

PRESIDENT

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION

ON THE

FY1987 ENERGY AND WATER DEVELOPMENT APPROPRIATIONS

BEFORE THE

ENERGY AND WATER DEVELOPMENT SUBCOMMITTEE

SENATE APPROPRIATIONS COMMITTEE

APRIL 21, 1986

Mr. Chairman and Members of the Subcommittee:

I am Bernard H. Falk, President of the National Electrical Manufacturers Association (NEMA). I want to thank you for this opportunity to present the concerns of NEMA and its members regarding the challenges and threats to the U.S. electrical power industry from unfair foreign trade practices.

The U.S. electrical power equipment manufacturing industry is the world leader in both technological advances and economic efficiency. Nevertheless, the industry is in a precarious condition. It has suffered, and continues to suffer, from unfair trading practices and unequal competitive access to overseas markets.

Foreign manufacturers of heavy electrical equipment have consistently been able to sell their products in the U.S., while their home markets have been effectively closed by their governments to our products. In many cases, this institutionalized protection acts as a subsidy, enabling the foreign companies to undercut U.S. goods in both the American and third country markets. This lack of equivalent competitive opportunities threatens the collapse of the U.S. electrical power equipment industry.

Last year the Congress took an important first step in redressing this inequity by increasing the "Buy American" differential for federal purchases of extra high voltage electric power equipment. Today, NEMA urges you to continue this 25 percent differential in the appropriation for fiscal year 1987.

As we have said before, NEMA does not come to this conclusion quickly, or without giving considerable thought to its implication. For nearly two decades, NEMA and its member companies have sought reciprocity and equivalent competitive opportunities for electrical power equipment. We have pursued this goal forcefully in every trade negotiation since the early 1960's. Despite these efforts, there is not even token reciprocity from other industrialized nations, regardless of whether or not their electric utilities are government owned. Electrical manufacturing companies in these nations, operating from a base of protected home markets, enjoy a built-in competitive advantage against U.S. companies both here and in third country markets.

Consider for example the outlook for the power transformer segment of the electrical equipment industry. Since the early 70's, the annual physical volume of shipments from U.S. companies is down 72 percent. U.S. employment in that industry dropped from 10,000 jobs in 1971 to 4000 in 1985. This represents a loss of skills and experience that may be irreplaceable.

In contrast, imports of foreign manufactured power transformers have increased rapidly, from 7 percent of the U.S. market in 1970-74, to 10 percent in 1975-79, to nearly 19 percent today.

What is causing this decline in market share for domestic producers? In September 1983, the General Accounting Office (GAO) found that unlike U.S. manufacturers, foreign manufacturers get significant government incentives to export their products, and that greatly aids them in their competition in the U.S. and other markets. In some cases, the GAO reported, foreign manufacturers are selling products both in the U.S. and in third country markets below their costs in order to maintain jobs and utilize their facilities. This is being done at the expense of U.S. skilled workers and the U.S. ability to produce heavy electrical equipment.

The GAO report says that between 1977 and 1981, 51 percent of the purchases of heavy electrical equipment by federal power agencies were from foreign manufacturers. In contrast, an Edison Electric Institute (EEI) survey conducted for the GAO reported that less than 15 percent of the purchases of investor-owned utilities were from foreign manufacturers.

The industry has not been idle in bringing this dilemma to the attention of the government. In 1972, the Office of Emergency Preparedness was informed about the problem in the extra high voltage (EHV) power circuit breaker segment and corrective action was requested. No action was taken, the government arguing that no U.S. manufacturer had dropped out of the business. Of the four manufacturers developing, designing and producing EHV breakers in the early 1970's, none is in business in 1986. Of the five manufacturers of EHV power transformers in the 1970's, only three remain in business. And of the four manufacturers of shunt reactors in the early 1970's, only one remains in business.

How best to respond is, of course, the question. The Congressionally-mandated section 302(d) report of the 1979 Trade Agreement sets forth a series of Administration proposals aimed at achieving equity and equivalent competitive access for this product sector. During the negotiations of the Government Procurement Code in the 1979 Tokyo Round, NEMA urged the inclusion of government entities which purchase electrical power equipment. The U.S. negotiators were unsuccessful in obtaining that inclusion because European governments would not agree. The proposals in the 302 report include expanding the entities covered by the Code through renegotiations and increasing the "Buy American" differential applicable to procurement. Renegotiation of the Code started in earnest in November 1983. As stated in the 1981 United States Trade Representative's Section 302 report, "if the United States is unable to obtain the agreement of other developed country Code signatories to expand their entity coverage by January 1, 1985, the USTR will recommend to Congress appropriate actions to achieve reciprocity." No progress has been made in the heavy electrical product sector and none is expected by most observers. I fully appreciate that renegotiation is multi-faceted and complex and I understand the Administration's position that renegotiation is the preferred approach, however, the renegotiation approach by itself offers no hope in achieving market access and reciprocity.

NEMA believes the long record of failure to achieve equivalent competitive opportunities and to open the markets of major competitors leaves the United States with only one course of action: to continue to exert pressure and impose progressively stronger countermeasures on such competition until equity and equivalent competitive opportunities are provided.

Based on the action which Congress took last year, the goal of achieving equivalency may be a bit closer. We are encouraged that there has been some movement by the federal utilities to implement the 25% differential in FY-86 procurement. We are also encouraged by recent government discussions to counter unfair and discriminatory procurement practices. Lastly, there has been some strengthening in the renegotiation of the Code to include utilities. The retention of the 25% differential is needed to continue the momentum and progress toward achieving equivalency.

Should the differential not have the desired effect of providing equivalent opportunities for U.S. manufacturers, stronger counter measures will be sought through legislation and through the upcoming new round of trade negotiations. In that regard, NEMA is actively involved in providing negotiation objectives and advice to our trade negotiators.

Therefore, bearing in mind that the objective is to induce foreign governments to truly open up their markets, NEMA urges that similar language be included in the fiscal 1987 legislation.

Thank you.

Statement of Michehl R. Gent,
President of North American Electric Reliability Council
Princeton, New Jersey

Mr. Chairman and Members of the Committee on Governmental Affairs, my name is Michehl R. Gent and I am president of the North American Electric Reliability Council. I appreciate this opportunity to discuss what the electric utility industry has done and is doing to address the threat of major interruptions to its facilities by natural disasters, sabotage, or terrorism.

The extreme sensitivity of this issue, as it relates to sabotage and terrorism, limits what I can present in an open hearing. From the very start of our deliberations, both the government representatives who approached us and the electric utility industry leaders involved in these initial discussions agreed that the success of our national electric security program demands a "quiet" activity removed from public attention.

I believe it is important that you know that the electric utility industry over its long history has an excellent record in responding to natural disasters. I also believe you should know that we have been very active for several years in addressing the threat of sabotage and terrorism and that we have developed a program to do just that through our National Electric Security Committee.

This electric security program is based on a cooperative, working relationship between the United States government and the electric utility industry in which the government has identified the issues to be addressed and industry has developed the solution -- one that it can implement and maintain. We think this approach can serve as a model for other energy industries and other industry sectors.

I can only present a "sanitized" version of our security program, because of its sensitive nature. Even with this limited description, we are concerned that it may draw unnecessary and unwanted attention -- an attention that can never be removed -- as well as stir the interest of other disruptive segments of society.

Who NERC is

The North American Electric Reliability Council (NERC) is the principal organization for coordinating, promoting, and communicating about reliability for North America's electric utilities. NERC was formed in 1968 in the aftermath of the November 9, 1965 Northeast Blackout.

The membership of NERC is quite unique. It is not a trade association or government-sponsored agency. It is a non-profit corporation whose owners are nine Regional Reliability Councils and one affiliate. NERC is actually a "federation" of these Regions. The members of the Regional Councils are individual electric utilities from all ownership segments of the industry -- investor-owned, federal, rural electric cooperatives, state, and municipal utilities. These utilities account for virtually all the electricity supplied in the United States, Canada, and the northern portion of Baja California, Mexico.

The activities of NERC are directed by its Board of Trustees. The Board is comprised of 27 electric utility executives including the Board's officers, two representatives from each Regional Council, and others as needed to assure at least one representative from a Canadian utility and at least two from each utility ownership segment. Meetings of the Board are attended by observers from the United States Department of Energy, the Federal Energy

Regulatory Commission, the National Energy Board of Canada, and from the utility industry's associations -- Edison Electric Institute, American Public Power Association, National Rural Electric Cooperative Association, and Canadian Electrical Association.

The technical activities of NERC are carried out by its Operating and Engineering Committees. Each Committee is comprised of managerial and high-level technical representatives from the Regional Councils. The people who make up these Committees and their subgroups provide unmatched expertise in the planning, engineering, and operating aspects of electric system reliability.

NERC's staff, located in Princeton, New Jersey, works with the Board, the Regional Councils, the Committees, and their subgroups to provide project coordination and support. The staff also is responsible for several data bases. The most well known is the Generating Availability Data System which houses the generating unit performance and outage event data of 174 electric utilities covering over 4,000 electric generating units. In addition, it also is responsible for the industry's loads and resources data base, which includes the hourly loads of most of the utilities in the U.S. and Canada, a Power Line Carrier data base, and data bases on major system disturbances and performance of the bulk electric systems.

Each Regional Council also has its own staff.

Reliability of the Bulk Electric System

The bulk electric systems in the United States are the most reliable in the world

-- a characteristic that is envied in other countries and should not be overlooked or dismissed lightly. By one measure, it is over three times more reliable than the bulk electric systems in the country with the next most reliable system and ten times more so than the bulk electric systems in the country with the third most reliable system. Major reasons for this are the design, operation, interconnection, and coordination exercised among the many utilities that come together to comprise the bulk electric systems of North America under the aegis of NERC.

Transmission Functions

The two major divisions of bulk electric systems are generation and transmission. The transmission system comprises the interconnected network of higher voltage and capacity electrical circuits. The function of a transmission system is twofold -- to provide a path for electricity from the points of generation to the major distribution points, and to connect the sources of electricity together so that they operate as an integrated whole. A source of electricity may be either a generating unit or a neighboring utility.

Other specific functions performed by transmission include providing a path for sales and purchases of electricity from other systems, providing a path for emergency support during an unexpected generating unit outage, and insuring the security of the overall bulk electric system. Some lines provide for one of these functions, while some lines may perform several functions simultaneously.

One characteristic of interconnected bulk electric systems is that all generators must operate in synchronism. Another is that at any instant in time the total output of these generators must equal the instantaneous electrical energy demands of all customers. In other words, the amount of energy leaving the transmission system (plus losses) always equals the amount entering.

Therefore, immediately following an outage of a transmission system component, power flows will redistribute themselves on the remaining lines. This occurs without regard to the power-carrying capabilities of the lines. Thus, overloads can occur.

Reliability dictates that bulk electric systems be designed and operated such that can they always accommodate the redistribution of flows resulting from the more likely outages. The ability of a system to survive disturbances is the aspect called "security."

Good Design and Operating Practice

Components of the transmission system can become unavailable for a number of reasons and in a very large number of combinations. Reliability considerations require sufficient redundancy and operating flexibility so that a "disturbance" will rarely result in unacceptable operating conditions, such as instability, overloads, inadequate voltage, or interruptions of customers. To meet those requirements, bulk electric systems must be designed and operated to:

- Assure that recovery from the more probable contingencies can be achieved without significant effect on customer service.

- Assure that the more severe, less probable contingencies (which include combinations of component outages) will not result in loss of synchronous operation, cascading outages, or the unintentional interruption of a large amount of customer load.

- Provide sufficient flexibility to allow for reliable operation during maintenance or repair.

- Ensure prompt restoration to normal operation following more severe, less probable disturbances.

The transmission network must be able to deliver the output of all generating units to the major points of distribution. The interconnections with adjacent utilities and the supporting internal transmission system must be sized to accommodate both routine and emergency transfers of energy between utilities. In addition, where not unduly constrained by environmental or economic factors, there must be sufficient redundancy of transmission lines such that no single transmission route will be depended on to carry a disproportionate share of any electricity transfer. Switching arrangements must be capable of isolating short circuits and quickly restoring the system to normal operation. A reliable system exhibits all of these characteristics.

"Routine" Emergencies

One key feature of these supply systems are their ability to transfer electricity between or among neighboring Regions in the event of an emergency. The nature of these "routine" emergencies vary from equipment failure, such as a generating unit, transmission line, transformer, or circuit breaker, to natural phenomena, such as a hurricane, flood, tornado, or earthquake, to man-made events, such as the coal strike of 1977-78. In each of these categories, the bulk electric systems were tested on numerous occasions and performed admirably, because of the flexibility built into their design, their operations, and the training of the people who operate them. We have learned our lessons of the past well and are up to meeting similar challenges in the future.

We recognize that all components of the bulk electric system can be considered important and the system may be vulnerable to failure of individual components. But, the systems' configurations have sufficient resiliency and redundancy that damage to many components can be absorbed and repaired or restored to service (with a sacrifice in reliability and flexibility) within weeks. For example, damaged circuit breakers can be bypassed and a switching arrangement can be revised; a damaged control house with damaged protective schemes can be restored, perhaps in several weeks; and if a system control center is destroyed, most utilities have back-up facilities available to maintain the basic system control functions. In nearly all cases, most of the customers can be jury-rigged back into the system within hours (at much lower severe reliability) until the damaged equipment can be replaced or repaired.

The New Element of Sabotage and Terrorism

The electric utility industry has worked hard for the past several years to design a workable program to strengthen our national electric security preparedness and make it both responsive to government needs and acceptable to the industry. From the very start of our deliberations, both government and industry agreed that the success of this national electric security program demands a "quiet" approach. We are very concerned about any attention focused on the electric utility industry's program through the media or otherwise as a result of open hearings. This public attention to the electric security preparedness program would be disruptive and it could never be removed. It also could draw the attention of other disruptive segments of society.

We believe that the basic approach the electric utility industry has taken with the government in this program, in which the government presents issues and the industry develops the solution, can serve as a model for other energy sectors. It also may serve as a model for other industry categories, such as transportation, hospitalization, housing, etc. This approach avoids a government-imposed solution that may be difficult for industry to implement and maintain.

Start of the Electric Security Program

The electric utility industry's program to deal with the possibility of sabotage and terrorism had its start following a reign of terrorism that began escalating in 1983. As a result, President Reagan appointed a task force headed by Vice President Bush to review the United State's program to combat terrorism. The task force's review of the current program to combat terrorism found the interagency system and the lead agency concept for dealing with incidents to be soundly conceived. However, the task force also determined that this system could be substantially enhanced through improved coordination.

In the area of energy emergency preparedness, the National Security Council (NSC) directed the Department of Energy (DOE) to establish a federal interagency group on energy vulnerability. The NSC recognized that energy systems are critical to the United State's domestic economy and national security. They were concerned that trained teams of foreign sponsored saboteurs could attack a number of key electric system facilities, and cause extended and widespread outages that would compromise our national security and seriously disrupt the domestic economy.

Several options were examined by DOE to develop a working relationship between the federal government and the industry. DOE determined that a federal advisory committee was not suitable, and consequently opted to work directly with NERC.

Discussions were held between high levels of government and the electric utility industry leadership that resulted in the Board of Trustees of the North American Electric Reliability Council unanimously approving a resolution establishing the National Electric Security Committee to develop a proposed program for (a) reviewing threats to the interconnected electric systems of the United States, (b) an organizational approach to analyze the nature and scope of such threats, (c) suggesting areas of consideration of viable and feasible enhancements to utility emergency preparedness, and (d) indicating strategies to address any appropriate improvements.

Over the course of about two and a half years, this special Committee of the Board, the National Electric Security Committee, has worked quietly and diligently to develop proposals that would be technically feasible solutions to reduce the vulnerability of interconnected bulk electric systems in the United States to state-sponsored, multisite sabotage and terrorism. These proposals in the form of a series of recommendations were presented to the NERC Board in July 1988; they were accepted by the Board in October. Some of the proposals have since been implemented and others are in various stages of review prior to implementation by the industry.

Since then, NERC has briefed the National Security Council, the Secretary of the Department of Energy, the President's National Science Advisor, and the Federal Emergency Management Agency on our National Electric Security Committee program.

The organizational chart for NERC and the NESC, which reports directly to NERC's Board of Trustees is attached. When NERC's Board of Trustees unanimously approved the formation of the NESC on January 6, 1987, it not only specified NESC's purpose as spelled out above, but also established guidelines for the Committee. It directed that NESC should: (a) Review all aspects of the interconnected facilities except those pertaining to nuclear, which are regulated by the NRC; and (b) Not develop a "blueprint," "hit list," or "critical facilities list" for the country which would be held in a central repository(s) and could fall into the hands of saboteurs or terrorists. It further directed that any identification of critical facilities that might be made should be kept internal and confidential by the utility on whose bulk electric system it is. The Board also directed that it shall provide exclusive policy guidance to the NESC.

Several key milestones in the progress of the NESC can be identified. These are:

January 7, 1986, Scottsdale, Arizona -- Representatives of the National Security Council attended the NERC Board of Trustee meeting and solicited NERC's assistance to develop a national electric utility security program.

March 7, 1986, Washington, D.C. -- Representatives of the NSC, DOE, and NERC met for a briefing on federal government concerns regarding the vulnerability of electric systems to sabotage and terrorism and to develop appropriate roles for NERC and DOE in organizing a program to address these concerns.

October 6, 1986, St. Louis, Missouri -- DOE, having filled key positions in its organization, developed a proposal for NERC's consideration. It attended the NERC Board meeting to officially present its proposal and request NERC's cooperations and participation. NERC authorized appointment of a Task Force on Electric Security. DOE's focus is on multisite sabotage and terrorism, not individual electric facility attacks, which the industry historically has shown it can handle.

November 19, 1986, Washington, D.C. -- NSC, DOE, and NERC's Task Force on Electric Security and its Advisory Working Group met so that DOE could elaborate on its proposals and NERC could decide on a course of action. DOE re-emphasized the need for "low-key" discussions on the program.

January 6, 1987, Scottsdale, Arizona -- The NERC Board unanimously approved a resolution creating the National Electric Security Committee. NERC reiterated that the program must be handled "quietly" and that NERC would interface with the Edison Electric Institute's Security Committee.

January 19, 1988, Chicago, Illinois -- NESC's three Working Groups met to rewrite their charters and action plans, as a result of a DOE Domestic Terrorism Threat briefing on November 2, 1987.

July 3, 1988, Coronado, California -- The NESC presented its report to the Board. The Board unanimously approved one recommendation for immediate implementation and held the remainder of the report for study and action at its next meeting.

October 10, 1988, New York, New York -- NERC's Board unanimously accepted the NESC report and approved the remaining recommendations.

Conclusion

I believe that this short "sanitized" description of what we have accomplished indicates that the electric utility industry has been very active over the last several years addressing the threat of major interruptions to its facilities by natural disasters, sabotage, or terrorism. We think we have an excellent record in responding to natural disasters. We also think we have shown that the industry has been actively developing a strong program to address the threat of foreign-state-sponsored multisite sabotage and terrorism.

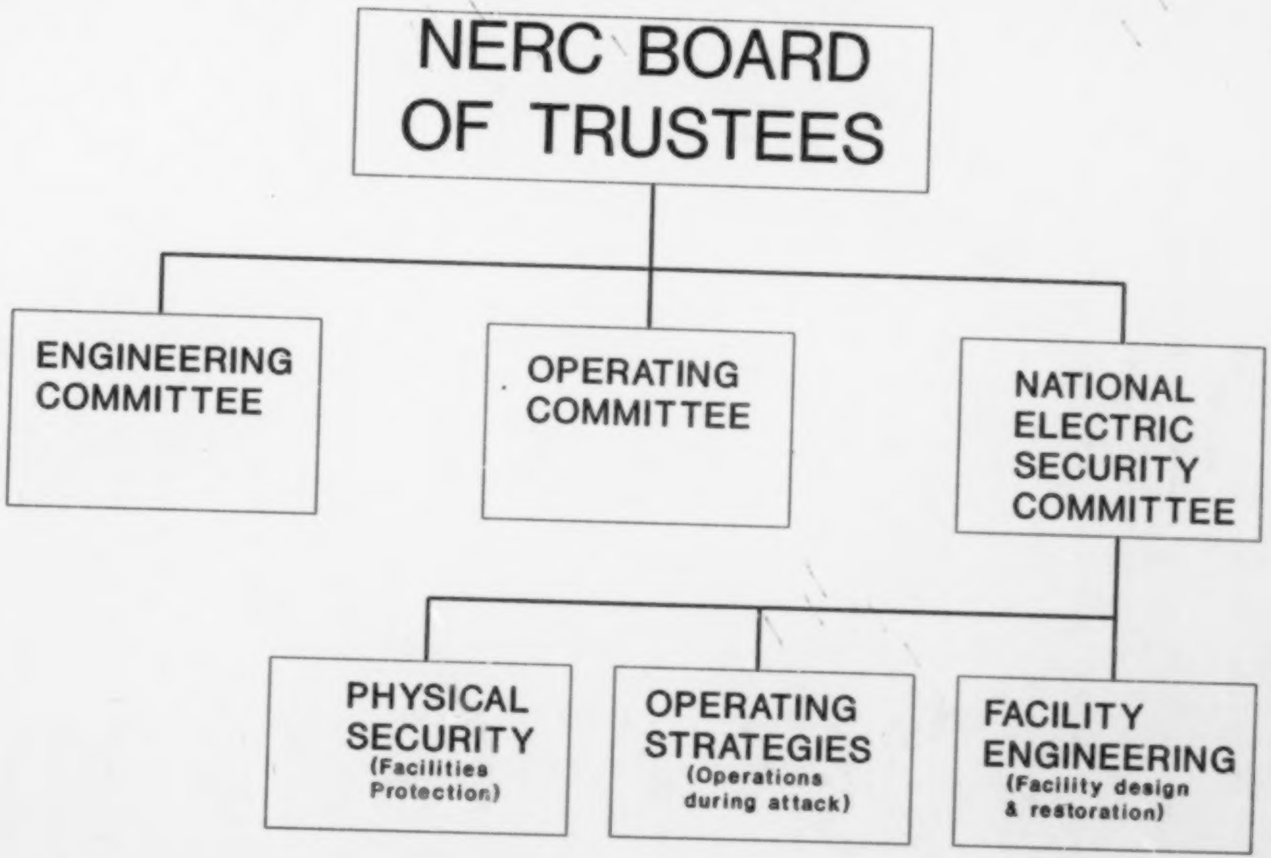
From the very start of our electric security program, both the government representatives and the industry leaders who worked on this program emphasized the need for a

From the very start of our electric security program, both the government representatives and the industry leaders who worked on this program emphasized the need for a "quiet" approach removed from public attention.

We do not question the oversight responsibility of the Senate Committee on Governmental Affairs regarding this subject. We do believe the Committee deserves the best input the electric utility industry can provide. We feel very strongly that an open hearing restricts the comments that the industry can make. Furthermore, we believe that open hearings can lead to sensationalizing by the media and others and can stir the interest of disruptive segments of society. This unnecessary attention can not be withdrawn at a later date.

We are more than willing to participate in closed hearings.

Finally, we think this program is unique in that it has been developed in cooperation with the federal government in which the government identifies the issues to be addressed and the electric utility industry develops the solution -- one that it can implement and maintain. This approach can serve as a model for other energy industries and other industry sectors.


NERC BOARD OF TRUSTEES
ENGINEERING COMMITTEE
OPERATING COMMITTEE
NATIONAL ELECTRIC SECURITY COMMITTEE
PHYSICAL SECURITY (Facilities Protection)
OPERATING STRATEGIES (Operations during attack)
FACILITY ENGINEERING (Facility design & restoration)

STATEMENT OF EDWARD V. BADOLATO
DEPUTY ASSISTANT SECRETARY FOR ENERGY EMERGENCIES
U.S. DEPARTMENT OF ENERGY

Mr. Chairman and Members of the Committee, I appreciate this opportunity to appear before you today to discuss energy emergency preparedness with particular emphasis on concerns that terrorists might attack the electric power grid and oil and natural gas pipelines.

As you may imagine, matters dealing with the vulnerabilities of our domestic energy systems are quite sensitive and must be handled delicately lest we create a shopping list for those who would do them harm. In view of the open nature of this hearing, I will limit my remarks to accommodate these sensitivities.

Introduction

The Department of Energy (DOE) has made substantial progress in supporting the goal of ensuring that customers have an adequate supply of energy at reasonable cost. DOE's (non-nuclear) energy emergency preparedness program seeks to reduce the Nation's vulnerability to energy supply disruptions and to enhance our ability to respond should a disruption occur. It is safe to say that the Unites States is better prepared than ever before to deter, as well as respond to, any energy supply emergency arising from foreign oil disruptions or from domestic incidents involving our basic energy industries.

However, the potential threat to energy supply systems from a multitude of causes ranging from natural disasters to terrorism requires vigilance and readiness. In 1986, the "Public Report of The Vice President's Task Force on Combating Terrorism" pointed out that:

> "Our vulnerability lies, ironically, in the strength of our open society and highly sophisticated infrastructure. Transportation, energy, communications, finance, industry, medicine, defense, diplomacy and government itself rely on intricate interrelated networks. Given these inherent vulnerabilities, and the fact that Americans are increasingly the targets of terrorist attacks outside the United States, it is apparent that a potentially serious domestic threat exists."

Mr. Oliver B. "Buck" Revell, Executive Assistant Director of the Federal Bureau of Investigation, addressed the International Association of Chiefs of Police on October 18, 1988, and appraised the current situation:

> "The United States ... is vulnerable to terrorist criminal activity. Potential terrorist support networks are in place in the United States and certain international terrorists have the motivation to commit terrorist acts ... the possibility of international terrorists committing acts in the United States continues to exist."

The Vice President's report and Mr. Revell's assessment provide a good baseline for working with the energy industry on the terrorism problem. While we are not aware of any serious terrorism activity directed at the U. S. energy infrastructure at present, industry and government awareness and acceptance of the serious potential is a major step in progressing toward energy emergency preparedness.

In June 1988, the National Security Adviser by memorandum to federal agencies and departments, established a functional approach to responding to emergencies which could adversely affect national security. Functional groups were specified in the areas of economics, energy, human services, legal and law enforcement, telecommunications, and transportation.

Each functional group is chaired by a lead department or agency which is responsible for identifying group members, emergency responsibilities, operating procedures and emergency actions, and for coordinating its emergency response activities with those of other functional groups. DOE is the lead department for the energy group.

President Reagan signed Executive Order 12656, entitled "Assignment of Emergency Preparedness Responsibilities," on November 18, 1988. Specific National Security Emergency Preparedness (NSEP) responsibilities and actions were assigned to departments and agencies using the same functional approach previously defined by the National Security Adviser. DOE's NSEP activities implement the President's Executive Order.

Over the past two years, DOE has taken decisive steps to substantially strengthen and reorganize the Nation's ability to respond to (non-nuclear) energy emergencies and ensure an adequate supply of energy at reasonable cost. Powerful new management tools incorporated departmental capabilities and crisis management systems into a structurally integrated framework for supporting U.S. preparedness. The Department has:

1. Developed procedures for and exercised an Energy Emergency Management System to facilitate its ability to respond to foreign or domestic energy emergencies.

2. Established the Federal Government's Interagency Group on Energy Vulnerability to assess energy vulnerabilities, evaluate response options, and analyze the consequences of emergency scenarios.

3. Developed a cooperative energy vulnerability assessment program to work with the energy industries (electric, oil, gas and coal) to study the domestic industry's facilities, security, and restoration capacity.

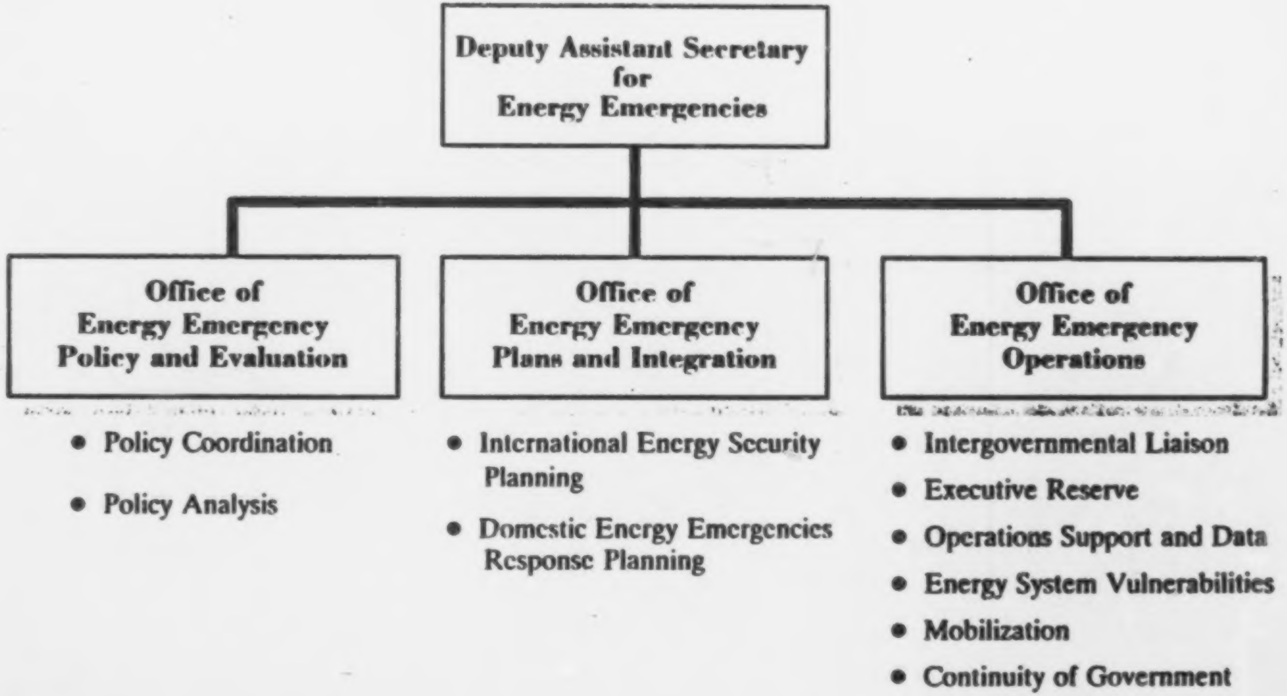
4. Revitalized the National Defense Executive Reserves--industry executives who will augment DOE's energy crisis management during emergencies--by recruiting members, establishing new training programs, and arranging for them to participate in the Department's tests and exercises.

Office of Energy Emergencies

DOE's Office of Energy Emergencies (OEE) has led a revitalized DOE effort to carry out its non-nuclear emergency preparedness strategies. OEE's FY 89 program budget totals about $6.2 million. This amount has remained essentially the same for the past five years, and is used mainly for staff direction. OEE's mission is to assure that adequate U.S. energy is available, at reasonable cost, to support national priorities during emergencies. As shown in Figure 1, three offices under my leadership carry out this mission.

Figure 1

Office of the Deputy Assistant Secretary for Energy Emergencies


Deputy Assistant Secretary
for
Energy Emergencies
Office of
Energy Emergency
Policy and Evaluation
• Policy Coordination
• Policy Analysis
Office of
Energy Emergency
Plans and Integration
• International Energy Security Planning
• Domestic Energy Emergencies Response Planning
Office of
Energy Emergency
Operations
• Intergovernmental Liaison
• Executive Reserve
• Operations Support and Data
• Energy System Vulnerabilities
• Mobilization
• Continuity of Government

1. The Office of Energy Emergency Policy and Evaluation: monitors, evaluates, incorporates, and disseminates energy emergency initiatives and developments in support of the OEE preparedness mission.

2. The Office of Energy Emergency Plans and Integration: develops energy emergency response plans that include the use of the Strategic Petroleum Reserve and the strengthening of commitments to the International Energy Agency and the North Atlantic Treaty Organization.

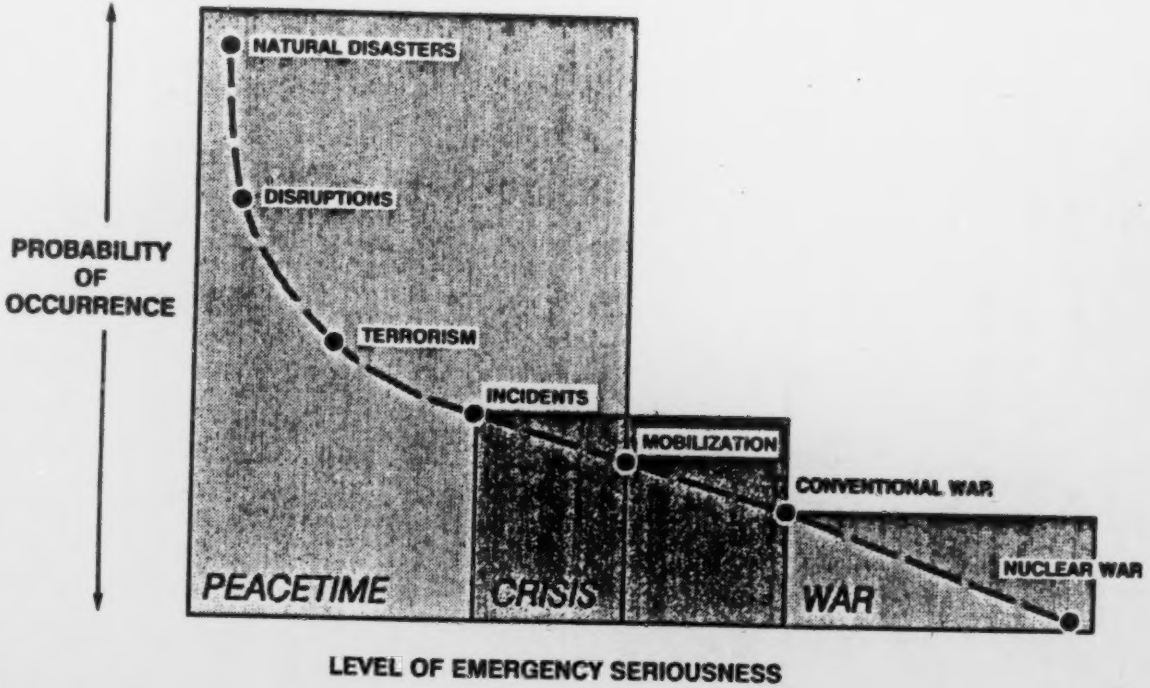
3. The Office of Energy Emergency Operations: undertakes efforts to ensure that the U.S. infrastructure (i.e., industry, state and local governments) is able to meet national priorities in the event of catastrophic and defense-related emergencies.

OEE uses the resources of other DOE offices and coordinates with other government agencies and industry for energy emergency planning and procedures. OEE resources must be available for use in responding to a broad spectrum of (non-nuclear) peacetime and wartime energy emergencies, as depicted in Figure 2. Natural disasters, political disruptions, terrorism, and sabotage have highest priority during peacetime. Crisis and wartime priorities involve energy preparedness for mobilization during conventional and nuclear war.

DOE's organizational commitment to energy emergency preparedness involves general and operational planning, procedures, budget and, most importantly, human resources. An effective crisis management system requires an

Figure 2

Energy Emergency Curve



experienced, mature, well-trained staff flexible enough to plan for and respond to a variety of emergency scenarios. OEE's 71 professional and support staff members include experts who have worked in the oil, gas, electric power, and coal industries, as well as economists, engineers, energy analysts, computer programmers, data processors, and administrative personnel. To ensure readiness for an unexpected emergency, the staff continually receives advanced training in technical and managerial skills. The emphasis on training and preparation for emergencies has been aimed at ensuring that DOE has a technically competent, though relatively small, staff that is well versed in energy crisis management policies and procedures and is capable of responding rapidly to emergencies.

OEE is concerned with both international and domestic energy emergencies and it focuses special attention on the vulnerabilities of each domestic energy system--electric power, oil, gas and coal. The nature and extent of international and domestic threats to energy security determine how OEE will carry out its emergency preparedness activities.

Domestic Energy Emergencies

Many natural and manmade events can disrupt the domestic energy supply system. Some emergencies, such as equipment failure or an act of vandalism, are routinely handled by industry, while larger problems that cannot be handled by industry or the States, such as the aftermath of a severe earthquake or potential multisite sabotage, may require Federal government coordination or assistance.

In the United States, multisite sabotage and terrorist incidents represent potential threats, but sabotage has not reached a level of severity to cause a major sustained outage. However, many third world countries, such as El Salvador, Peru, Chile, Colombia, Mozambique, Afghanistan, and Guatemala, have experienced substantial energy system disruptions because of terrorism.

Terrorist organizations also have repeatedly attacked energy facilities throughout the world. In the past, these attacks generally were poorly designed and executed, but a disturbing trend in these attacks is an increase in the level of technology used and an improvement in their planning. This may portend more effective attacks.

Energy-related terrorism in the United States would be a particularly significant threat in a time of national defense mobilization. The Soviet Union has an unconventional warfare capability, Spetsnaz units, to which it has assigned the mission of crippling the West's industrial infrastructure, particularly its vulnerable energy systems, before an outbreak of hostilities. Although the main Spetsnaz target appears to be Western Europe, the potential for such action in the United States cannot be ruled out. However, even in the absence of a superpower confrontation, it is possible that potential third world adversaries could sponsor attacks on the energy infrastructure in the United States, so OEE is working with industry to mitigate this potential threat.

Vulnerability Mitigation

A clear focus has been established for DOE's vulnerability assessment program in which our first priority is electric power services, which are vital to economic and social stability and to national security. Because the electric utility industry (Figure 3) is so spread out, it appears to be the most vulnerable of all U.S. energy systems. More than 144,000 miles (230 kV and above) of bulk power transmission lines--many stretching over remote, unprotected areas--connect the Nation's powerplants to consumers. Worldwide, transmission lines have been the most common targets for terrorists. In fact, books and articles are available in the U.S. which describe techniques for toppling transmission towers and destroying transmission line insulators by rifle fire. The rifle fire method was recently used to destroy 25 insulators on a transmission line in Texas.

Substations, with their vital transformers and circuit breakers, are the final critical link in the distribution system and are the next system components most exposed to hostile actions. Generating stations and critical fuel and water supplies also are vulnerable. The vulnerability of the electric supply system is exacerbated because the repair or replacement of many substation and powerplant components may take weeks or months.

The petroleum industry (Figure 4) has second priority in U.S. domestic emergency preparedness policy for coping with vulnerability. The industry's principal points of vulnerability are pipelines, refineries, and storage facilities. However, the storage and transportation flexibility of the petroleum industry makes it less vulnerable than the electric power industry.

Figure 3

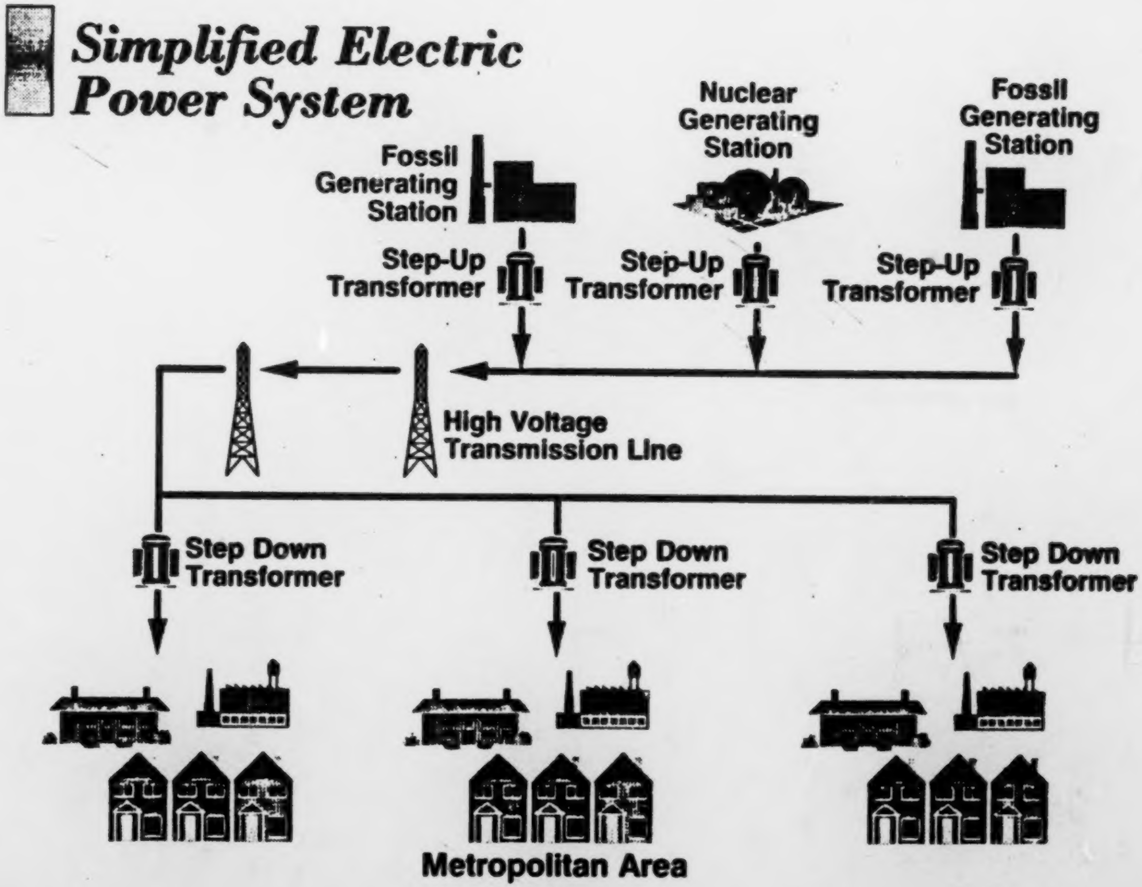
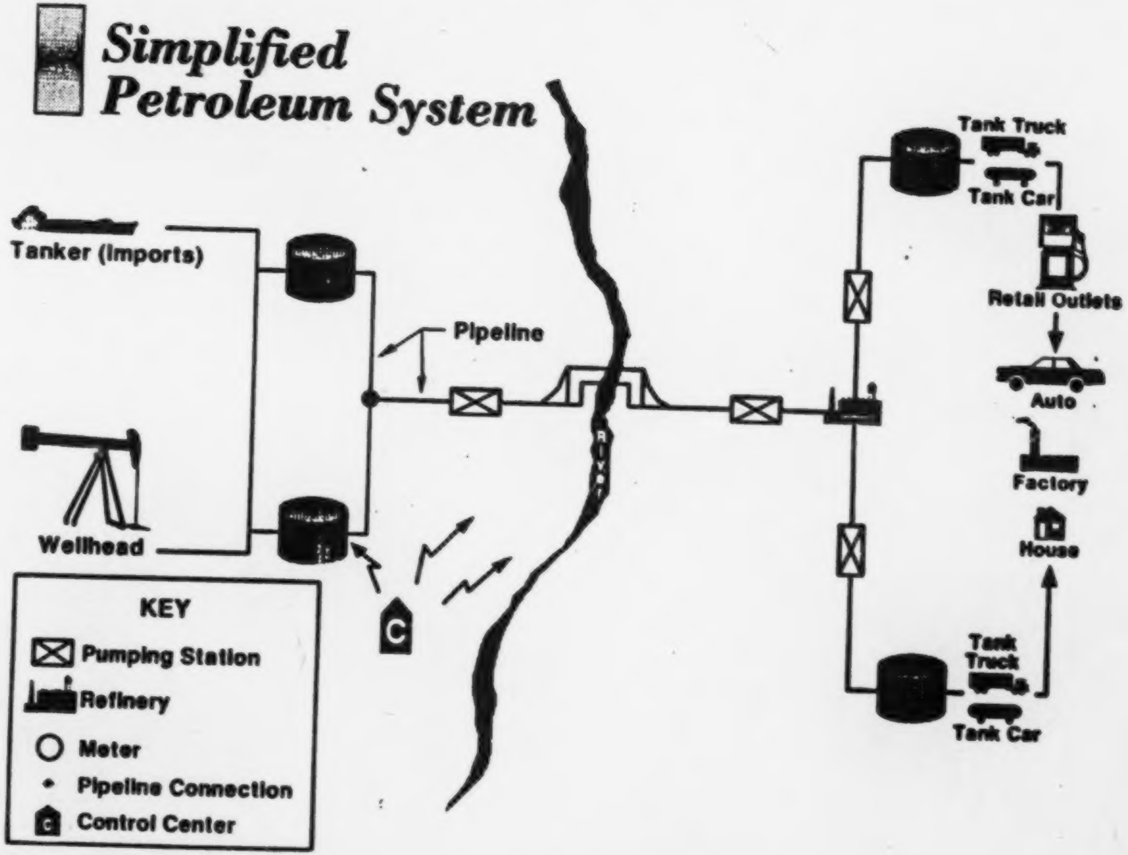

Simplified Electric
Power System
Fossil Generating Station
Nuclear Generating Station
Fossil Generating Station
Step-Up Transformer
Step-Up Transformer
Step-Up Transformer
High Voltage Transmission Line
Step Down Transformer
Step Down Transformer
Step Down Transformer
Metropolitan Area

Figure 4


Simplified Petroleum System
Tanker (Imports)
Wellhead
Pipeline
River
C
Tank Truck
Tank Car
Retail Outlets
Auto
Factory
House
Tank Truck
Tank Car
KEY
Pumping Station
Refinery
Meter
Pipeline Connection
Control Center

For example, crude oil and petroleum products can be rerouted around damaged areas as well as imported from other countries and transported by various methods, including pipeline, water, rail, and fuel trucks.

The natural gas industry (Figure 5) is DOE's third domestic priority. The most vulnerable components are critical pipeline interconnections, river crossings, compressor stations, and city gate stations. The transmission and distribution system for natural gas, which consists of more than 1 million miles of pipeline, constitutes such a complex and redundant set of targets that it reduces the opportunity for inflicting crippling damage. In addition, the dual fuel capacity of many industries is a safeguard against the effects of a major disruption to the gas system.

Although coal supplies 30 percent of our energy, the dispersed nature of its transportation network from mine to generating plants makes it unlikely that even a large hostile action could have a significant effect on the Nation's coal and its transportation network. Rail or barge coal transportation to electric generating plants may pose some vulnerability to a hostile act, but history shows that labor strikes have caused the most disruption to the coal industry.

A DOE vulnerability mitigation program (Figure 6), consisting of four phases, has been developed and clearly described to industry in various meetings around the country. That program, described below, is designed to recognize and utilize industry's technical expertise on what is operationally best for their systems and the Federal Government's responsibility for national security.

Figure 5

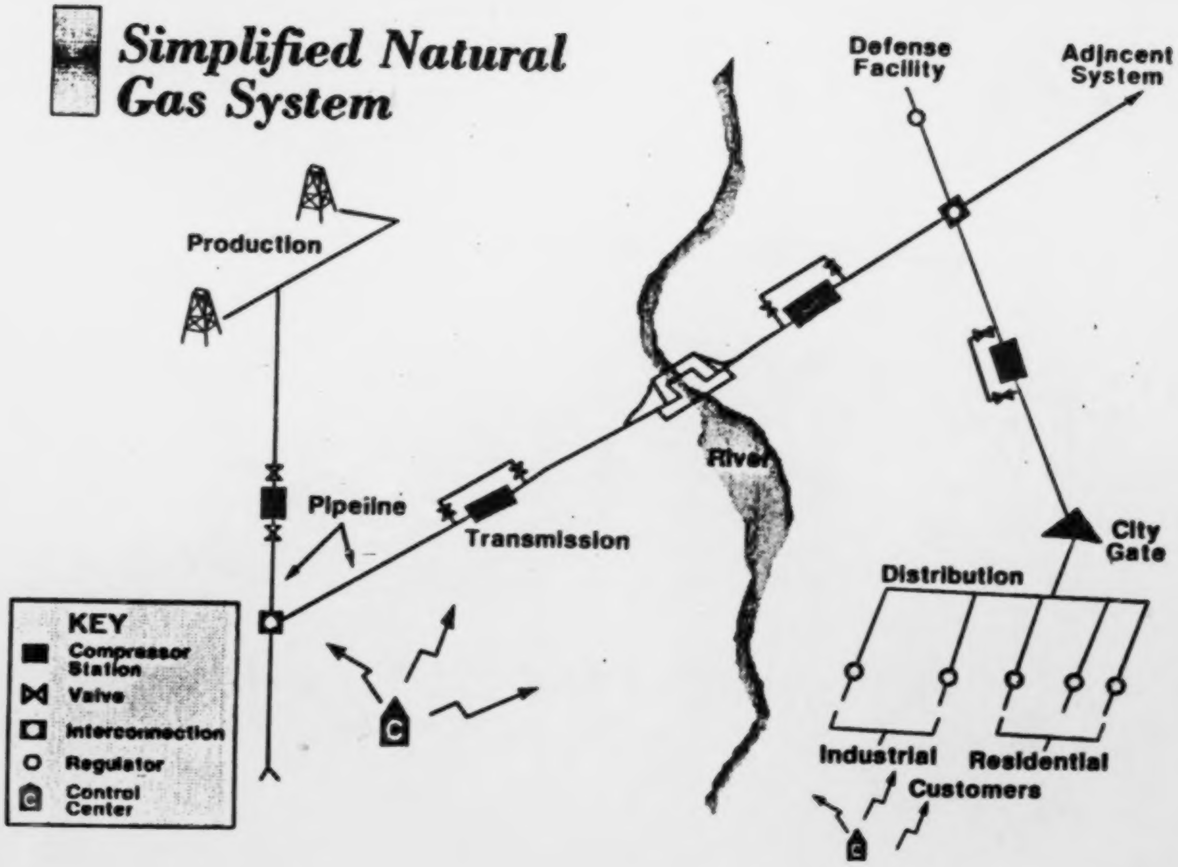
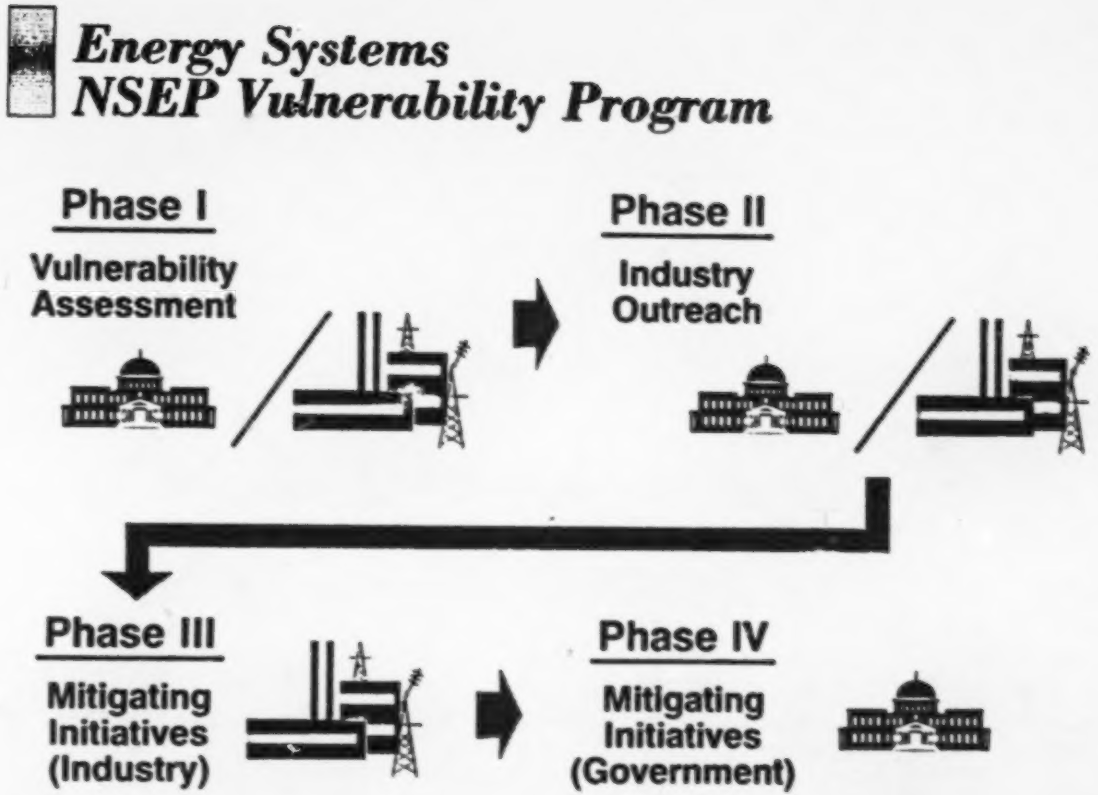

Simplified Natural Gas System
Production
Pipeline
Transmission
River
Defense Facility
Adjacent System
City Gate
Distribution
Industrial
Residential
Customers
KEY
Compressor Station
Valve
Interconnection
Regulator
Control Center
C

Figure 6



Energy Systems NSEP Vulnerability Program

Phase I

Vulnerability Assessment

Phase II

Industry Outreach

Phase III

Mitigating Initiatives (Industry)

Phase IV

Mitigating Initiatives (Government)

Phase I: Vulnerability Assessment. In-house case studies and simulations to assess the vulnerabilities of candidate energy systems;

Phase II: Industry Outreach. Outreach to industry owners and operators to advise of discovered vulnerabilities and to obtain cooperation;

Phase III: Industry Mitigating Initiatives. Introspective vulnerability assessments by system owners and operators to determine enhancements which may be in accordance with normal business objectives; and

Phase IV: Government Mitigating Initiatives. Assessments of remaining vulnerabilities and judgments as to whether they constitute an unacceptable risk to national security and, if so, the kinds of remedies which may be warranted.

Because most energy supply systems are privately owned and operated, industry has a key role to play in assessing risks and taking preventive measures. DOE supports industry by providing a program to address the vulnerability of each domestic energy system, the time and resources required to restore operations, should disruptions occur, and cost-effective ways to mitigate threats to these energy systems. The program encompasses in-house studies and simulations to determine the nature of the vulnerabilities; an industry outreach program to highlight potential vulnerabilities; and monitoring remedial actions to determine the sufficiency of industry actions.

In line with the above risk assessment program, DOE has made vulnerability assessments of electric power systems, the Strategic Petroleum Reserve, petroleum refineries, petroleum pipelines, offshore oil and gas facilities, and natural gas transmission pipeline systems.

The North American Electric Reliability Council (NERC) has led the way in the vulnerability program. The Secretary of Energy, with the concurrence of the National Security Council, requested a study by NERC of vulnerabilities in the electric power industry. NERC has completed a year long study and its member utilities have begun to implement the study's recommendations to mitigate vulnerabilities.

DOE has initiated similar outreach activities in the petroleum and natural gas industries.

Responding to Energy Emergencies

Among the important management tools which have so effectively strengthened the Department's emergency preparedness strategy, DOE has developed a generalized emergency response process called the Energy Emergency Management System (EEMS). This system provides a structurally integrated framework that supports systematic decision-making in response to any energy emergency, whether in the electric power, oil, gas, or coal industries, or in the event of an international or domestic energy crisis. The EEMS is organized to assess the nature and extent of an energy emergency and, by drawing upon the total support activities and expertise of DOE, to develop response options.

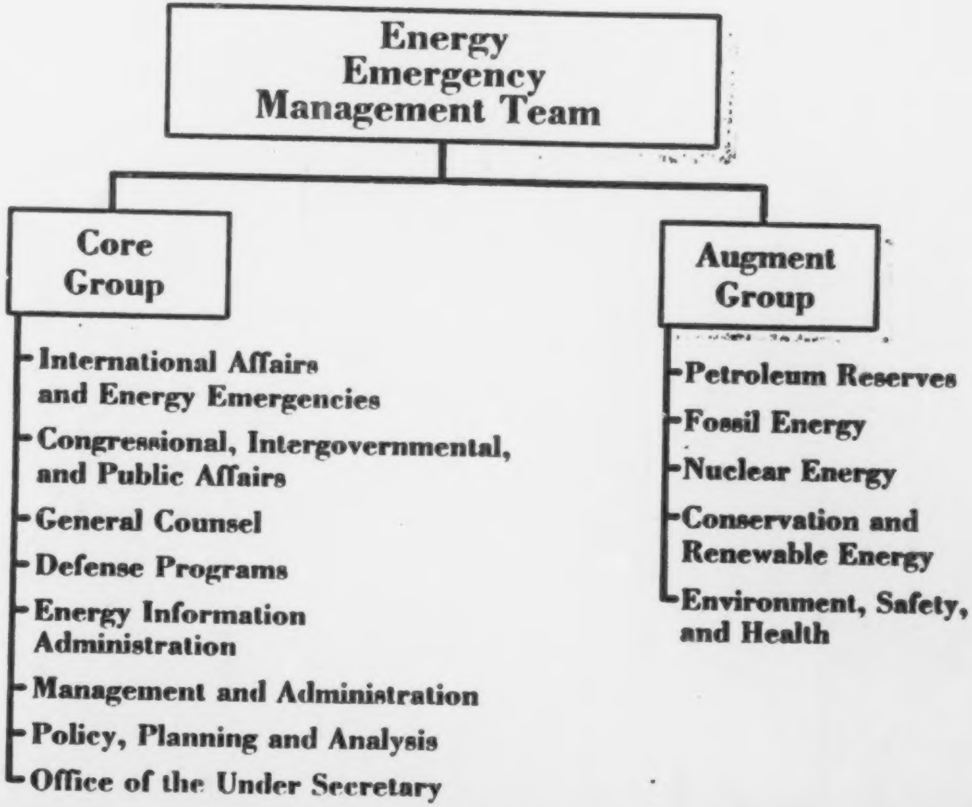
Besides establishing response procedures for each principal energy type, the EEMS process also is designed to respond to a variety of possible emergency scenarios, such as an oil supply disruption caused by international incidents, defense mobilization, major natural disasters, energy system sabotage, major accidents involving energy systems, and economic damage during labor strikes.

In the draft DOE Order 5500.5 "Energy Emergency Planning and Management," the EEMS concept is defined and the policies and procedures for administering EEMS are established, as are the general criteria for developing and coordinating DOE's energy emergency planning activities. As the non-nuclear energy component of DOE's overall Emergency Management System, the order describes the EEMS organizational relationships and integrates its concepts of operations into the emergency processes of the Department. During 1987, the EEMS process was successfully tested in a large-scale exercise.

The key organizational component of EEMS is the Energy Emergency Management Team (EEMT), a cadre of departmental experts chaired by the Deputy Assistant Secretary for Energy Emergencies. Figure 7 illustrates the EEMT structure. As DOE's principal internal energy crisis management body, the EEMT has met numerous times, providing the Secretary of Energy with status briefings and projections on such subjects as the likely effects of pipeline damage by earthquakes on energy supplies, the Persian Gulf U.S.S. Stark incident, oil tanker mining activities off Kuwait, the Red River washout of an oil pipeline in the southwestern U.S. and the impact of the 1988 drought on energy supplies.

In typical situation meetings, the EEMT is provided with an up-to-date detailed intelligence briefing, an analysis of the effects of an incident on

Figure 7


Energy Emergency Management Team
Core Group
International Affairs and Energy Emergencies
Congressional, Intergovernmental, and Public Affairs
General Counsel
Defense Programs
Energy Information Administration
Management and Administration
Policy, Planning and Analysis
Office of the Under Secretary
Augment Group
Petroleum Reserves
Fossil Energy
Nuclear Energy
Conservation and Renewable Energy
Environment, Safety, and Health

energy supplies, and recommendations for appropriate response actions. In addition to real-life, incident-oriented meetings, the EEMT has tested its procedural proficiency in various exercises.

Figure 8 illustrates the operational concept of EEMS. The continuum begins with routine monitoring of the energy situation to determine whether it is necessary to activate the EEMT and the EEMS process. Next, the situation is analyzed, various response options are considered, and recommendations are made and implemented. Each step in the flow of activities allows for termination of the EEMS process if it is no longer necessary, or recycling if the emergency continues.

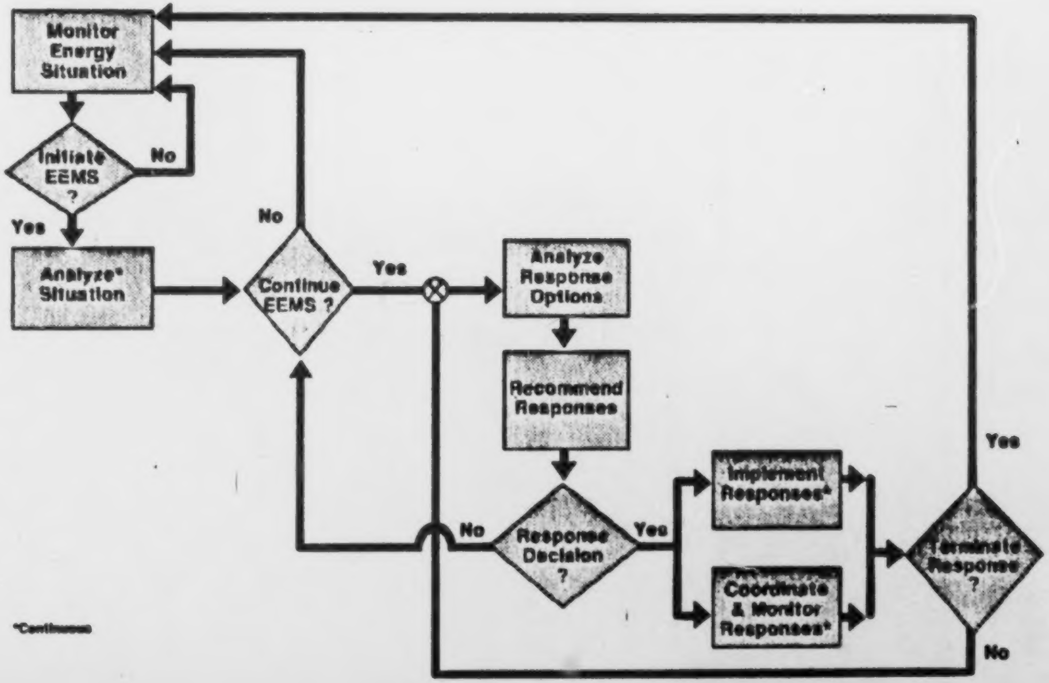
Interagency Group on Energy Vulnerability

Concern for national security emergency preparedness prompted the National Security Council to establish, a DOE-chaired Interagency Group on Energy Vulnerability (IG-EV) (Figure 9) in 1987. The objective was to enhance energy emergency preparedness policy and the response process. This forum is currently under review by the Administration.

The IG-EV is currently an important adjunct of the national energy crisis management process. The group consists of senior representatives, generally at the Assistant Secretary level, with national energy emergency preparedness responsibilities from various departments and agencies. The purpose of this group is to assess energy vulnerabilities, evaluate energy emergency data and projections, consider response options, and analyze the consequences of possible emergency scenarios and response actions.

Figure 8

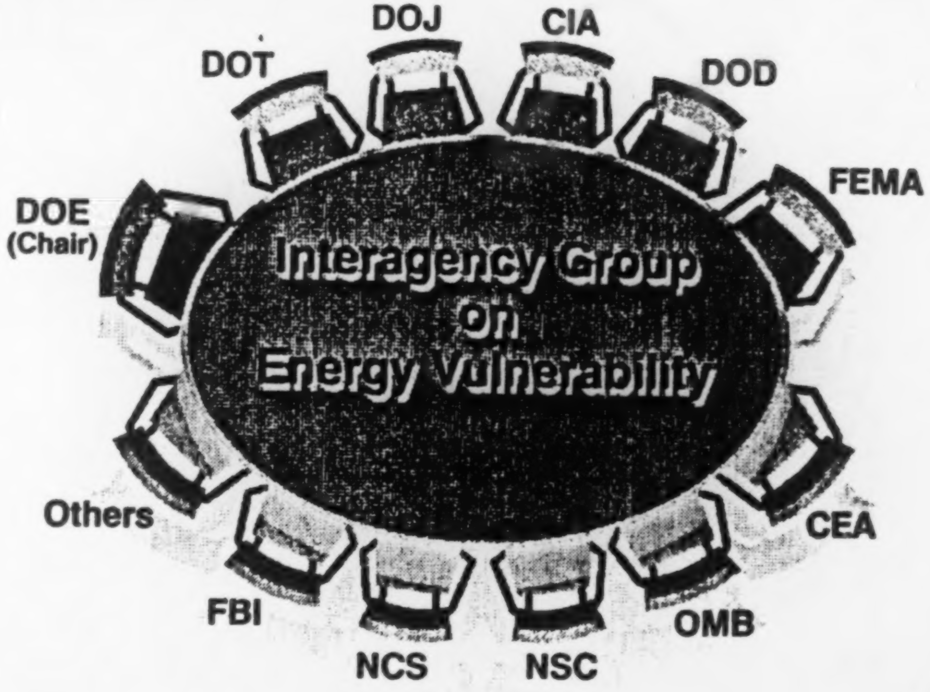
Energy Emergency Management System: Simplified Diagram


Monitor Energy Situation
Initiate EEMS ?
No
Yes
Analyze* Situation
Continue EEMS ?
No
Yes
Analyze Response Options
Recommend Responses
Response Decision ?
No
Yes
Implement Responses*
Coordinate & Monitor Responses*
Terminate Response ?
Yes
No

*Continuous

Figure 9

Intergovernmental Coordination for Energy Emergencies


Interagency Group on Energy Vulnerability
DOE (Chair)
DOT
DOJ
CIA
DOD
FEMA
CEA
OMB
NSC
NCS
FBI
Others

The IG-EV draws upon the supporting activities of the three subgroups shown in Figure 10. The major functions of each subgroup follow:

1. The Subgroup on Energy Vulnerability Assessment has the important task of examining the vulnerability of U. S. energy systems to nonroutine disruptions that may affect national security. The group may then consider actions that could be implemented in advance to reduce the likelihood of or lessen the effect of disruptions that may occur.

2. The Subgroup on Database and Projections analyzes the effects of the changing energy marketplace.

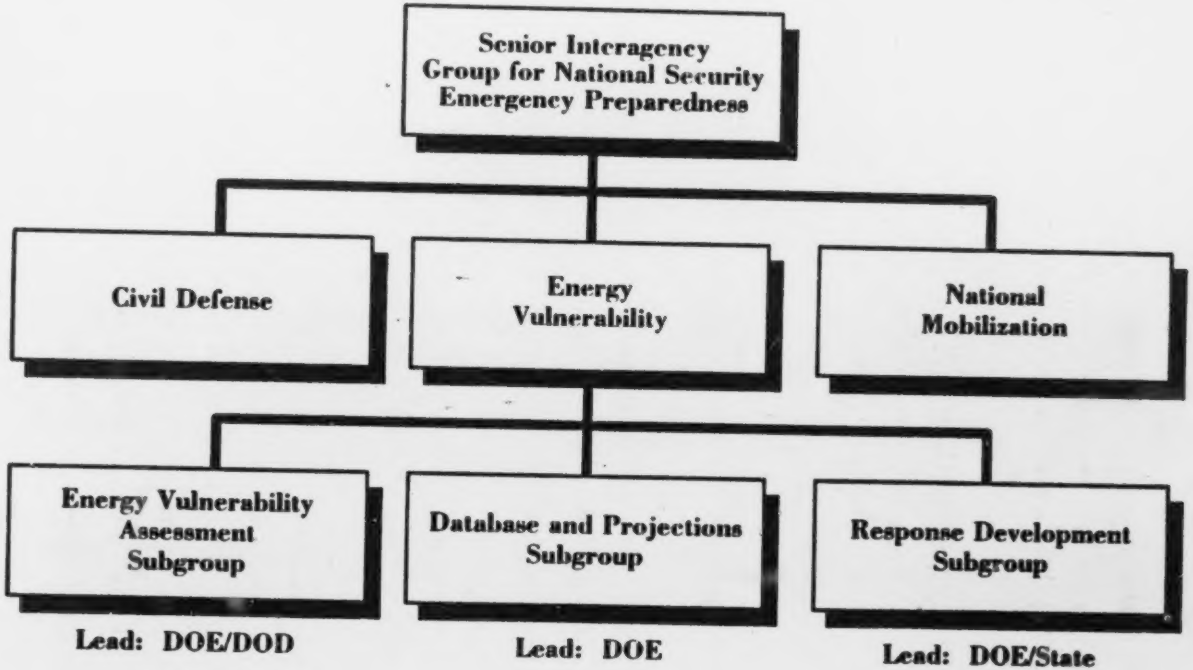
3. The Subgroup on Response Development evaluates response measures and international activities that could be implemented during an energy emergency.

A complete report of the activities and accomplishments of the IG-EV and its Subgroups was published in January 1989 and is attached: "Report of the Interagency Group on Energy Vulnerability, November 1986 - November 1988".

National Defense Executive Reserves

As a part of its effort to expand government/industry cooperation in preparing for energy emergencies, DOE has revitalized its National Defense Executive Reserves (NDER) program. DOE develops, trains, and maintains NDER units

Figure 10


Senior Interagency Group for National Security Emergency Preparedness
Civil Defense
Energy Vulnerability
National Mobilization
Energy Vulnerability Assessment Subgroup
Database and Projections Subgroup
Response Development Subgroup
Lead: DOE/DOD
Lead: DOE
Lead: DOE/State

composed of energy industry professionals to augment DOE's energy management activity during national security emergencies. These executives from the electric power, coal, natural gas, and petroleum industries voluntarily agree to serve in the Federal Government during such emergencies. DOE assigns unit members specific positions, initiates security investigations and subsequent clearances, and then trains them in government procedures and emergency functions. DOE envisions that the executive reservists could help assess damage, evaluate energy systems' supply capability, and coordinate with industry on supply and repair priorities. They would also coordinate with other Federal agencies on overall Federal energy priorities.

As part of DOE's NDER training program, new reservists attend orientation and training developed by the Lawrence Livermore National Laboratory and held at the DOE Central Training Academy facilities located in Albuquerque, New Mexico. Alternate locations will be used for some training sessions to facilitate attendance. Some members receive additional training by participating in DOE's exercise and simulation program.

Accelerated recruitment for executive reservists has resulted in bringing the Executive Reserve staff of the Electric Power unit to 50% and Solid Fuels to 80% of the staffing goal. DOE plans to have these two NDER units concentrate on recruiting and filling their regional and state liaison positions. In addition, DOE is continuing an aggressive recruitment program for the Natural Gas Executive Reserves by holding regional meetings to organize and staff that unit.

Energy Security

Former Energy Secretary Herrington has stated: "Government/industry cooperation is vital to the national security of this Nation." DOE is planning to enhance Government and industry cooperation in energy security by facilitating industry's access to DOE's expertise and physical security training programs. The Department has provided a special training program to members of the security force for the Trans Alaskan Pipeline System (TAPS). The DOE is now working to provide the energy industry with the DOE-developed Automated Vulnerability Assessment System, a computer program for determining security requirements of energy facilities. This system provides a standarized way to evaluate facility security by drawing upon a database reflecting years of barrier and safeguards testing by the National Laboratories.

Threat Notification System

Because prevention or deterrence is a far more effective way to deal with energy emergencies than suffering the physical or economic damage of a disruption to energy supply systems, DOE has initiated a notification system to alert the energy industry of threatening situations. The notification, or Threat Advisory, consists of a message that describes, in general, a threat that could lead to aggressive actions; for example, the Iranian reaction to the reflagging of Persian Gulf vessels. The receiving organizations, such as NERC, the American Petroleum Institute (API), the National Coal Association (NCA), the American Gas Association (AGA), and the Interstate Natural Gas

Association of America (INGA) cooperate by retransmitting these advisories to their industry members. DOE is pleased that the FBI is planning to take over this responsibility as part of its comprehensive counterterrorism program.

Classified Communications with Industry Security Officials

In order to provide the opportunity for more specific planning for the physical security of U.S. energy systems, security clearances have been requested for several senior security officials of the U.S. electric utility industry. The clearances will facilitate classified discussions on topics such as techniques used, or planned, by terrorists to sabotage electric power facilities; federal counterterrorism programs as they relate to the industry; and briefings on terrorist organizations deemed potential threats by the intelligence community.

With the background information provided, these officials can provide leadership to the industry toward adopting responsive physical security planning and operating practices.

On-Shore Availability of Major Replacement Components

Significant numbers of critical components (e.g., transformers, circuit breakers) may be needed on short notice in the event of a severe emergency or multisite sabotage against energy facilities. Major changes are occurring in the availability of such components as the U.S. heavy equipment manufacturing base continues to downsize. DOE is closely monitoring the on-shore availability of such components, along with the availability of special transportation equipment (e.g., Schnabel railroad cars) required to move large heavy equipment on short notice.

Electric Power Supply Adequacy and Reliability

DOE maintains a current understanding of the status of electric power supplies through analysis, communication, and coordination. An important element of long-term energy emergency preparedness is DOE's annual analysis and publication of the national electric power supply outlook. Basic data for this analysis comes from North American Electric Reliability Council (NERC) and its nine Regional Reliability Councils and covers the period from the present to ten years into the future.

DOE requires utilities to report significant electric reliability problems as they occur. Such problems include major power outages, load reductions, fuel supply problems and acts of sabotage against the bulk power supply system. Constant contact with the industry, so that action can be initiated promptly when serious problems develop, is ensured by a 24 hour a day, 7 days a week, Alert Coordination Officer duty system staffed by OEE personnel.

In order to coordinate closely with the industry on electric reliability matters, DOE representatives attend NERC Board of Trustees and Engineering Committee meetings in observer status.

Key Asset Protection Program

The Department of Defense (DoD) conducts a Key Asset Protection Program (KAPP), intended to protect important industrial assets from sabotage during times of increased international tension or national emergency. Some industry-owned energy facilities are considered key assets. DOE is cooperating with industry and DoD in this program.

U.S. - Canada Memorandum of Understanding

U.S. national security relies on Canadian energy facilities in some areas. Likewise, Canadian national security sometimes depends on U.S. energy facilities. In 1988, the U.S. and Canada signed a Memorandum of Understanding which provides for cooperation in identifying and protecting key facilities involved in these interdependencies.

Foreign Energy Emergency Technical Assistance

On occasion, the State Department requests technical assistance from DOE on behalf of foreign governments which are experiencing energy emergencies.

In 1988, DOE provided such assistance to the government of Colombia's national oil company (ECOPETROL) which experienced repeated sabotage of an important crude oil pipeline.

This year, DOE has provided technical assistance to the government of Argentina, which is experiencing rotating electric power blackouts because of equipment failures and a drought.

Exercises

DOE has an intensive program to maintain readiness for energy emergencies. OEE has conducted or participated in a number of exercises related to energy emergencies involving U.S. electricity, natural gas and petroleum supplies. These exercises test the soundness of emergency plans and coordination, reveal the causes and dynamics of different types of emergencies, enable participants to gain an understanding of factors which influence the outcome, and develop networks of future value to participants. Numerous Federal, state, local and industry officials have participated.

The following is a representative list of the energy emergency exercises conducted:

- Curtailment of oil exports from the Persian Gulf;
- Regional electricity outage caused by multisite sabotage;
- Regional electricity shortage caused by load growth and inadequate generating capacity expansion;
- National gas pipeline disruption caused by multisite sabotage;
- Petroleum pipeline sabotage;
- Offshore oil and gas platform and pipeline sabotage;

- Large metropolitan area (San Francisco) energy shortages in a partial mobilization and sabotage situation;
- Largescale earthquake damage;
- Statewide (California and Iowa) energy emergencies;
- Energy emergencies and response plans for the northeast, south, midwest and western regions of the U.S.; and
- Energy supply and demand in partial and full-scale mobilization for national defense.

Energy Emergency Decision Support System

Data handling is a critical component of DOE's capability to respond to an energy emergency. Energy emergencies are complex events that significantly affect other systems--communication, transportation, defense capabilities, modern food production--that are basic to our Nation's well-being. DOE uses a computerized energy emergency preparedness Decision Support System (DSS) for analyzing data for use in its crisis management decision-making process.

The DSS, which was developed by the Office of Energy Emergencies, can access detailed energy and economic data from various sources, such as the Energy Information Administration (EIA) and commercial data bases. Using these data, OEE staff can develop scenario analyses and briefing material from current data and incorporate the results in models, simulations, and graphic displays.

The system's memory also must be able to incorporate the results of past exercises and simulations for future application. In addition, the system must be capable of using information critical to top decision makers on current political and economic conditions, with options and solutions for a particular emergency. The Office of Energy Emergencies is working with contractors and several of the National Laboratories to enhance DSS capabilities by developing a menu system, coding structure and standardizing the access and implementation procedures for the staff to interconnect with other systems.

Office Automation for Energy Emergencies

To facilitate general operations and improve data communications among the staff, other DOE offices and outside organizations, OEE is providing personal computers to certain staff members. This enables staff to use microcomputers to exchange information in several electronic media networks, as well as to maintain electronic mail communications with the State Energy Offices, the DOE National Defense Executive Reserves, and other key energy emergency contacts.

State/Local Outreach

The past eighteen months has seen a revitalization of federal-state-industry energy emergency preparedness cooperation. In large measure this is due to DOE's efforts to open lines of communication and coordination, and to the responsiveness of state and industry emergency planners to these initiatives.

OEE has formed a state steering group which is used as a forum to surface various issues, discuss them, and thereby work towards consensus regarding state energy emergency preparedness programs.

In cooperation with the Strom Thurmond Institute of Government and Public Affairs at Clemson University, seminars were planned to share information and train personnel. Four regional seminars, which included energy emergency simulations, have been conducted. Almost 40 states participated, along with dozens of industry representatives.

In response to a request from OEE, the National Research Council of the National Academy of Sciences formed the Committee on State and Federal Roles in Emergency Preparedness. The committee was charged with providing an independent assessment of the current arrangements among Federal, state and industrial units for planning for and managing emergencies, and with recommending actions that DOE and the states could take to improve the level of emergency preparedness. These recommendations have been received in a report entitled "State and Federal Roles in Energy Emergency Preparedness."

NSTAC: Telecommunications/Energy Interdependencies

In its September 1986 Oversight Report, the Telecommunications System Survivability (TSS) Task Force of the National Security Telecommunications Advisory Committee (NSTAC) concluded that the telecommunications industry is heavily dependent on commercial electrical power to maintain day-to-day operations. Thus, if the electric power grid were rendered inoperable for some reason, the communications industry may be unable to operate at current levels, since it would be dependent on its back-up power systems. These systems generally operate for short periods of time, which would not suffice in the event of substantial damage to the power grid. Therefore, with its dependence on commercial power and limited back-up power capabilities, the telecommunications industry is vulnerable to a coordinated attack on electric utility systems.

Concerned about the potentially catastrophic results of an extended power outage, in February 1987 the TSS Task Force recommended that the NSTAC request that the Department of Energy address the problem of survivable power.

In April 1987, the TSS Task Force briefed the Energy Vulnerability Assessment Subgroup (EVAS) of the Interagency Group on Energy Vulnerability, and established its own subgroup on power. In July 1988, the Power Subgroup of the TSS Task Force formally offered to assist the EVAS in its review of energy vulnerability and its relationship to telecommunications.

In his October 1987 reply to the report of the NSTAC, President Reagan indicated that "The Department of Energy will work closely with the NSTAC and the National Communications System to ensure that the concerns of the telecommunications industry are addressed within the framework of ongoing national security emergency preparedness initiatives."

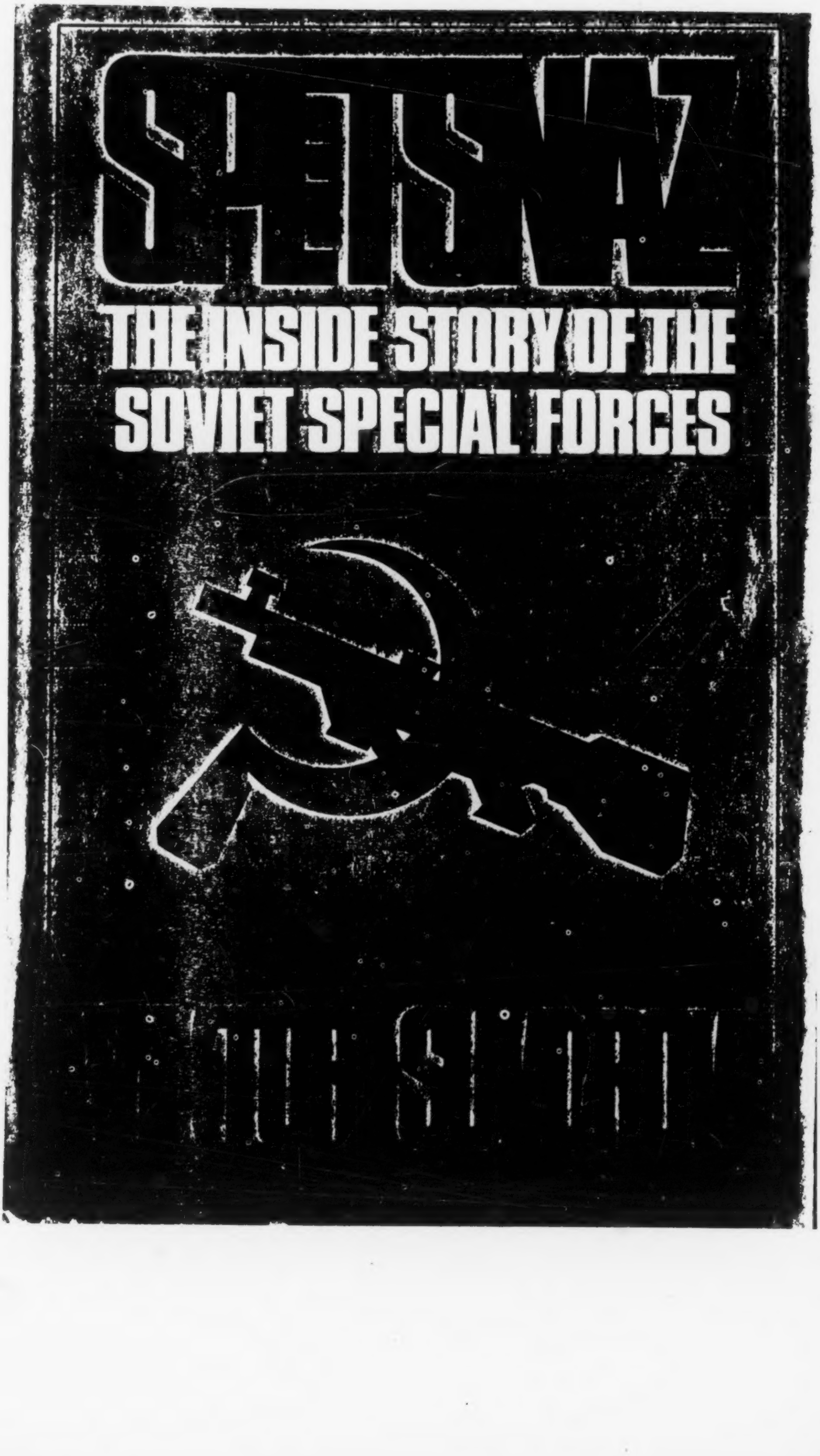
I have described earlier in this testimony the initiative undertaken by the North American Electric Reliability Council (NERC) at the request of the National Security Council and the Department of Energy. That initiative, together with DOE's vulnerability work under EVAS auspices, led in June 1988 to expanding the membership of the TSS Power Subgroup to include members of the electric power industry. In September 1988, the TSS Power Subgroup was elevated to the status of Energy Task Force, NSTAC. Presently, the Energy Task Force has members from both the telecommunications and electric power industries and has developed a program to identify mutual interdependencies between the two network systems. These interdependencies will be examined carefully under simulated emergency conditions. Vulnerabilities deemed to be unacceptably high will be targeted for further analysis and development of recommendations to mitigate their possible adverse impact on national security.

In another initiative, DOE is working with the TSS Power Subgroup on issues arising from a draft EPA regulation affecting underground storage of emergency fuel supplies at telecommunications facilities. There is concern that telecommunications firms may reduce emergency preparedness by replacing underground tanks with smaller above ground tanks, or forgo emergency fuel stocks altogether at some sites.

Outlook

Over the past several years decisive action on many fronts has been taken to enhance national security emergency preparedness. Unprecedented participation by government and industry in assessing and mitigating energy system vulnerabilities has been achieved. The Department of Energy, through its Office of Energy Emergencies, plans to continue its priority program to mitigate energy supply system vulnerabilities.

This concludes my prepared testimony. I will be happy to answer your questions.


SPETSNAZ
THE INSIDE STORY OF THE
SOVIET SPECIAL FORCES

Copyright © 1987 Viktor Suvorov

First American Edition, 1988.

All rights reserved.

Printed in the United States of America.

ISBN 0-393-02614-0

W.W. Norton & Company, Inc. 500 Fifth Avenue, New York, N.Y. 10110
W.W. Norton & Company Ltd., 37 Great Russell Street, London WC1B 3NU

1 2 3 4 5 6 7 8 9 0

Chapter 15

Spetsnaz's First World War

I was standing on the top of an enormous skyscraper in New York when I saw King Kong. The huge gorilla surveyed Manhattan triumphantly from a dizzy height. Of course I knew it wasn't real. But there was something both frightening and symbolic in that huge black figure.

I learnt later that the gorilla was a rubber one, that it had been decided to celebrate the fiftieth anniversary of the showing of the first film about King Kong by creating a gigantic inflatable model of the beast and placing it high above New York. The rubber monster was hauled up and swayed about in the wind. From the technical point of view the operation had been a real triumph by the engineers and workmen who had taken part in it. But it was not an entire success. The monster turned out to be too huge, with the result that holes appeared in its body through which the air could escape. So the gigantic muscular frame quickly collapsed into a shapeless bag. They had to pump more air into it, but the harder they pumped the bigger the holes became and the quicker the air escaped from the monster. So they had to keep on pumping. . . .

The Communist leaders have also created a rubber monster and have hauled it up to a dizzy height. The monster is known as the Union of Soviet Socialist Republics, and the Soviet leaders are faced with a dilemma: to expand or to decline rapidly and become a flabby sack. It is interesting to note that the Soviet Union became a superpower in the course of the most destructive war in the history of civilisation, in spite of the fact that it suffered the greatest loss of life and the greatest destruction on its own territory. It has become a military superpower and perhaps war is essential for its existence.

I do not know how or when World War Three will start. I do not know exactly how the Soviet high command plans to make use of *spetsnaz* in that war: the first world war in which *spetsnaz* will be a major contributor. I do not wish to predict the future. In this chapter I shall describe how *spetsnaz* will be used at the beginning of that war as I imagine it. It is not my task to describe what will happen. But I can describe what *might happen*.

■ ■ ■

The last month of peace, as in other wars, has an almost palpable air of crisis about it. Incidents, accidents, small disasters add to the tension. Two trains collide on a railway bridge in Cologne because the signalling system is out of order. The bridge is seriously damaged and there can be no traffic over it for the next two months.

In the port of Rotterdam a Polish supertanker bursts into flames. Because of an error by the captain the tanker is far too close to the oil storage tanks on the shore, and the burning oil spreads around the harbour. For two weeks fire brigades summoned from practically the whole country fight an heroic battle with the flames. The port suffers tremendous losses. The fire appears to have spread at a quite incredible speed, and some experts are of the opinion that the Polish tanker was not the only cause of the fire, that the fire broke out simultaneously in many places.

In the Panama Canal the *Varna*, a Bulgarian freighter loaded with heavy containers, rams the lock gates by mistake. Experts reckoned that the ship should have remained afloat, but for some reason she sinks there and then. To reopen the canal could well take many months. The Bulgarian government sends its apologies and declares itself ready to pay for all the work involved.

In Washington, as the President's helicopter is taking off, several shots are fired at it from sniper's rifles. The helicopter is only slightly damaged and the crew succeed in bringing it down again safely. No one in the craft is hurt. Responsibility for the attack is claimed by a previously unknown organisation calling itself 'Revenge for Vietnam'.

There is a terrorist explosion at Vienna airport.

A group of unidentified men attack the territory of the British military base in Cyprus with mortars.

A serious accident takes place on the most important oil pipeline in Alaska. The pumping stations break down and the flow of oil falls to a trickle.

In West Germany there are several unsuccessful attempts on the lives of American generals.

In the North Sea the biggest of the British oil rigs tips over and sinks. The precise reason for this is not established, although experts believe that corrosion of main supports is the culprit.

In the United States an epidemic of some unidentified disease breaks out and spreads rapidly. It seems to affect port areas particularly, such as San Francisco, Boston, Charleston, Seattle, Norfolk and Philadelphia.

There are explosions practically every day in Paris. The main targets are the government districts, communication centres and military headquarters. At the same time terrible forest fires are raging in the South of France.

All these operations – because of course none of these events is an accident – and others like them are known officially in the GRU as the 'preparatory period', and unofficially as the 'overture'. The overture is a series of large and small operations the purpose of which is, before actual military operations begin, to weaken the enemy's morale, create an atmosphere of general suspicion, fear and uncertainty, and divert the attention of the enemy's armies and police forces to a huge number of different targets, each of which may be the object of the next attack.

The overture is carried by agents of the secret services of the Soviet satellite countries and by mercenaries recruited by intermediaries. The principal method employed at this stage is 'grey terror', that is, a kind of terror which is not conducted in the name of the Soviet Union. The Soviet secret services do not at this stage leave their visiting cards, or leave other people's cards. The terror is carried out in the name of already existing extremist groups not connected in any way with the Soviet Union, or in the name of fictitious organisations.

The GRU reckons that in this period its operations should be regarded as natural disasters, actions by forces beyond human control, mistakes committed by people, or as terrorist acts by organisations not connected with the Soviet Union.

The terrorist acts carried out in the course of the 'overture' require very few people, very few weapons and little equipment. In some cases all that may be needed is one man who has as a weapon nothing more than a screwdriver, a box of matches or a glass ampoule. Some of the operations can have catastrophic consequences. For example, an epidemic of an infectious disease at seven of the most important naval bases in the West could have the effect of halving the combined naval might of the Soviet Union's enemies.

The 'overture' could last from several weeks to several months, gradually gathering force and embracing fresh regions. At the same time the GUSM would become involved. Photographs compromising a NATO chief appear on the front pages of Western newspapers. A scandal explodes. It appears that some of the NATO people have been having meetings with high-ranking Soviet diplomats and handing over top secret papers. All efforts to refute the story only fuel the fire. The public demands the immediate dismissal of NATO'S chiefs and a detailed enquiry. Fresh details about the affair are published in the papers and the scandal increases in scope. At that moment the KGB and GRU can take out and dust off a tremendous quantity of material and put it into circulation. The main victims now are the people whom the Soviets had tried to recruit but failed. Now carefully edited and annotated materials get into the hands of the press. Soviet Intelligence has tried to recruit thousands, even tens of thousands, of people in its time. They include young lieutenants who have now become generals and third secretaries who have now become ambassadors. All of them rejected Soviet efforts to recruit them, and now Soviet Intelligence avenges their refusal. The number of scandalous affairs increases. The nations discover to their surprise that there are very few people to be trusted. The Soviet intelligence service has nothing to lose if the press gets hold of material showing that it tried to recruit a French general, without saying how the attempt ended. It has even less to lose on the eve of war. That is why the newspapers are full of demands for investigations and reports of resignations, dismissals and suicides. The best way of killing a general is to kill him with his own hands.

There is a marked increase in the strength of the peace movement. In many countries there are continual demands to make the country neutral and not to support American foreign policy, which has been discredited. At this point the 'grey terror' gathers scope and strength and in the last days of peace reaches its peak.

From the first moment of the first day of war the main forces of *spetsnaz* go into action. From then on the terror is conducted in the name of the Soviet Union and of the Communist leadership: 'red terror'.

But between the 'grey' and the 'red' terror there may be an intermediate period – the 'pink' terror, when active military operations have not yet begun and there is still peace, but when some of the best *spetsnaz* units have already gone into action. The situation is complicated by the fact that, on the one hand, Soviet fighting units are already in battle, but that, on the other hand, they are not yet operating in the name of the Soviet Union. This is an exceptionally risky moment for the Soviet high command. But he who risks nothing gains nothing. The Soviet commanders want to gain a great deal, and so are ready to risk a lot. A great deal has of course been done to reduce the level of risk. Only a relatively small number of *spetsnaz* troops take part in the 'pink' terror, but they are the best people in *spetsnaz* – professional athletes of Olympic class. Everything has been done to make sure that not one of them should fall into the hands of the enemy before the outbreak of war. A great deal has also been done to ensure that, if one of them should fall into enemy hands at that moment, it would be very difficult to establish his connection with any country whatsoever.

The 'pink' terror may continue for no more than a few hours. But those are the most important hours and minutes – the very last hours and minutes of peace. It is very important that those hours and minutes should be spoilt for the enemy and used for the maximum advantage to the Soviet side. It must be pointed out that the 'pink' terror may not be carried out at all. It is used only when there is absolute certainty of the success of the operations and equal certainty that the enemy will not be able in the remaining hours and minutes to assess the situation correctly and strike the first pre-emptive blow.

■ ■ ■

For Soviet Communists the month of August has a special significance. It was in August that the First World War began, which resulted in revolutions in Russia, Germany and Hungary. In August 1939 Georgi Zhukov succeeded in doing something that no one before him had managed to do: with a sudden blow he routed a group of Japanese forces in the Far East. It is possible that that blow had very far-reaching consequences: Japan decided against attacking the Soviet Union and chose to advance in other directions. Also in August 1939 a pact was signed in the Kremlin which opened the flood gates for the Second World War, as a result of which the USSR became a super-power. In August 1945 the Soviet Union carried out a treacherous attack on Japan and Manchuria. In the course of three weeks of intensive operations huge territories roughly equal in area and population to Eastern Europe were 'liberated'. In August 1961 the Soviet Union built the Berlin Wall, in violation of international agreements it had signed. In August 1968 the Soviet Army 'liberated' Czechoslovakia and, to its great surprise, did not meet with any opposition from the West.

Suppose the Soviet Communists again choose August for starting a war. . . .

* * *

On 12 August, at 0558 local time, a van comes to a halt on the vast empty parking lot in front of a supermarket in Washington. Three men open the doors of the van, roll out the fuselage of a light aircraft and attach its wings. A minute later its motor bursts into life. The plane takes off and disappears into the sky. It has no pilot. It is controlled by radio with the aid of very simple instruments, only slightly more complicated than those used by model aircraft enthusiasts. The plane climbs to about 200 metres and immediately begins to descend in the direction of the White House. A minute later a mighty explosion shakes the capital of the United States. The screaming of sirens on police cars, fire engines and ambulances fills the city.

Three minutes later a second plane sweeps across the centre of the city and there is a second explosion in the place where the White House once stood. The second plane has taken off from a section of highway under construction, and has a quite different control system. Two cars with radio beacons in them have been left earlier in the middle of the city. The beacons have switched on automatically a few seconds before the plane's take-off. The automatic pilot is guided by the two beacons and starts to descend according to a previously worked-out trajectory. The second plane has been sent off by a second group operating independently of the first one.

It was a simple plan: if the first plane did not destroy the White House the second would. If the first plane did destroy the White House then a few minutes later all the heads of the Washington police would be near where the explosion had taken place. The second plane would kill many of them.

At 0606 all radio and television channels interrupt their normal programmes and report the destruction of the White House and the possible death of the President of the United States.

At 0613 the programme known as *Good Morning America* is interrupted and the Vice-President of the USA appears. He announces a staggering piece of news: there has been an attempt to seize power in the country on the part of the leaders of the armed forces. The President of the United States has been killed. The Vice-President appeals to everyone in the armed forces to remain where they are and not to carry out any orders from senior officers for the next twenty-four hours, because the orders would be issued by traitors shortly to be removed from their posts and arrested.

Soon afterwards many television channels across the country cease transmitting. . . .

■ ■ ■

The Soviet military leaders know that if it doesn't prove possible to destroy the President of the United States in peacetime, it will be practically impossible to do so at a time of crisis. The President will be in an underground, or airborne, command post, somewhere extremely inaccessible and extremely well guarded.

Consequently the leaders, while not abandoning attempts to kill the President (for which purpose several groups of assassins with every kind of weapon, including anti-aircraft missiles, have been dropped in the country), decide to carry out an operation aimed at causing panic and confusion. If it proves impossible to kill the President then they will have to reduce his capacity to rule the country and its armed forces at the most critical moment.

To carry out this task the Soviets have secretly transferred to Washington a *spetsnaz* company from the first *spetsnaz* regiment at the strategic level. A large part of the company is made up of women. The entire complement of the company is professional athletes of Olympic standard. It has taken several months to transfer the whole company to Washington. The athletes have arrived in the guise of security men, drivers and technicians working in the Soviet embassy and other Soviet establishments, and their weapons and equipment have been brought in in containers covered by diplomatic privilege. The company has been split into eight groups to carry out its mission. Each group has its own organisation, structure, weapons and equipment. To carry out their tasks some of the groups will have to make contact with secret agents recruited a long time previously by the GRU *rezidentura*.

On 11 August the GRU *rezident* in Washington, a major-general known by the code-name of 'Mudry' (officially a civilian and a high-ranking diplomat) receives an encyphered telegram consisting of one single word – 'Yes'. On the *rezident*'s orders the *spetsnaz* company leave their places of work. Some of them simply go back home. Some are transported secretly in the boots of their cars by GRU officers and dropped in the woods round the city, in empty underground garages and other secluded places.

The group commanders gather their groups together in previously agreed places and set about carrying out their tasks.

Group No. 1 consists of three men and the group is backed up by one secret agent. The agent works as a mechanic at an airport. In his spare time he builds flying models of aircraft of various sizes. This particular model was designed by the best Soviet aircraft designers and put together in America from spares bought in the open market. The agent himself does not play any part in the operation. A van containing a light radio-guided aircraft and its separate wings has been standing in his garage for some months. What the aircraft is for and to whom it belongs the agent does not know. He only knows that someone has the keys to the garage and that that person can at any moment come and take the van along with the aircraft. In the middle of the night the *spetsnaz* group drives the van out into the forest where they take the explosive charges from a secret hiding place and prepare the plane for flight. At dawn the van is standing in the deserted parking lot.

Group No. 2 is doing roughly the same at that time. But this group has three agents working for it, two of whom have left their cars with radio beacons parked in precisely defined spots in the centre of the city.

Group No. 3 consists of fifteen *spetsnaz* men and five experts from the REB *osnaz*. They are all wearing police uniforms. At night the group kidnaps the director of a television company and his family. Leaving the family at home as hostages guarded by three *spetsnaz* men, the rest of the group make their way to the studios, capturing two more highly placed officials on their way, also as hostages; but without giving cause for noise or panic among the staff. Then, with guns threatening them and supervised by Soviet electronics experts, the director and his assistants insert, instead of the usual advertising programme, a video cassette which the commander of the group has given him. The video cassette has been made up in advance in the Soviet Union. The role of the Vice-President is played by an actor.

The Soviet high command knows that it is very difficult to cut into American military channels. If it is at all possible, then at best it will be possible to do no more than overhear conversations or interrupt them. It is practically impossible to use them for transmitting false orders at the strategic level. That is why it is decided to make use of the civilian television network: it is difficult to get into a television studio, but it is possible and there are many to choose from. Operations are carried out simultaneously in several different cities against various TV companies. If the operation succeeds in only one city it will not matter – millions of people will be disoriented at the most critical moment.

The operational plan has provided that, just after the 'Vice-President' has spoken several retransmitters will be destroyed by other *spetsnaz* groups and one of the American communication satellites will be shot down 'by mistake' by a Soviet satellite. This is intended to deprive the President and the real Vice-President of the opportunity to refute the false declaration.

But events do not go entirely according to plan. The President succeeds in addressing the people and issuing a denial of the report. After the television network throughout America has suffered such major damage, the radio immediately becomes the principal means of communication. Radio commentators produce different commentaries about what is happening. The majority of them report that it is difficult to say which report is genuine and which was false, but that the only fact about which there is no doubt is that the White House has been destroyed.

At the moment when all these events are taking place in

Washington another *spetsnaz* company from the same regiment is ordered by the GRU *rezident* in New York to carry out the same operation but on a much larger scale. They do not make use of radio-guided aircraft, but seize two television studios and one radio studio which they use for transmitting the same false report. Five other *spetsnaz* groups emerge from official Soviet offices and make open, armed attacks on underground cables and some radio and TV transmitting and receiving aerials. They manage to damage them and also some transformer stations, as a result of which millions of TV screens go blank.

A few hours later *spetsnaz* detachment I-M-7 of 120 men lands in New York harbour from a freighter sailing under a Liberian flag. Using its fire-power the detachment makes its way to the nearest subway station and, splitting into small groups and seizing a train with hostages, sets about destroying the underground communications of the city.

In the area around the berths of America's huge aircraft-carriers and nuclear submarines in Norfolk, several mini-subs are discovered, as well as underwater saboteurs with aqualungs.

In Alaska eighteen different places are recorded where small groups have tried to land from Soviet naval vessels, submarines and aircraft. Some of the groups have been destroyed as they landed, others have managed to get back to their ships or, after landing successfully, hidden in the forests.

Spetsnaz detachment I-S-7 consisting of eighty-two men lands on the coast of Mexico, immediately commandeers private cars, and the next night, using their fire-power and new mobility, cross the United States border.

Small *spetsnaz* groups land and use routes and methods employed by illegal immigrants, while others make use of paths and methods used by drug dealers.

Islands and the military installations on them are more vulnerable to sabotage operations, and at the same moment *spetsnaz* groups are landing on Okinawa and Guam, on Diego Garcia, in Greenland and dozens of other islands on which the West has bases.

■ ■ ■

Spetsnaz group 2-S-13 has spent three weeks aboard a small Soviet fishing vessel fishing close to the shores of Ireland. On receiving the signal '393939' the ship's captain gives the order to cut the nets, switch off the radio, radar and navigation lights and set course at top speed for the shores of Great Britain.

In darkness two light speed-boats are lowered from the side of the ship. They are big enough to take the whole group. In the first boat is the group commander, a lieutenant with the code-name of 'Shakespeare', a radio operator, a machine-gunner and two snipers. In the second boat is the deputy group commander, a junior lieutenant with the code-name 'Poet', two soldiers with flame-throwers and two snipers. Each man has a supply of food for three days, which is supposed to be used only in the event of being pursued for a long period. For general purposes the group has to obtain its food independently, as best it can. The group also includes two huge German shepherd dogs.

After landing the group the little fishing vessel, still without lights or radio, puts out into the open sea. The ship's captain is hoping to hide away in a neutral port in Ireland. If the vessel is stopped at sea by a British naval patrol the captain and his crew have nothing to fear: the dangerous passengers have left the fishing boat and all traces of their presence on it have already been removed.

'Shakespeare's' group lands on a tiny beach close to Little Haven. The landing place has been chosen long ago, and very well chosen: the beach is shut in on three sides by huge cliffs, so that even in daytime it is impossible to see from a distance what is going on on the beach itself.

At the same time as 'Shakespeare' four other *spetsnaz* groups are going ashore in different places two or three kilometres apart. Operating independently of each other, these four groups arrive by different routes at the little village of Brawdy and at 3.30 in the morning they make a simultaneous attack from different directions on a large building belonging to the United States Navy. According to reports received by the GRU, hundreds, and possibly thousands, of acoustic listening posts have been set up in the region of the Atlantic Ocean. The underwater cables from these posts come together at Brawdy where hundreds of American experts analyse with the aid of a computer a huge amount of information about the movement of submarines and surface ships all over the North Atlantic. According to the GRU's information similar establishments have been set up in Antigua in the Azores, in Hofn and Keflavik in Iceland, in Hawaii and on Guam. The GRU's commanding officers are aware that their information about Brawdy may not be accurate. But the decision has been taken to attack and destroy the Brawdy monitoring station and all the others as well. The four attacking groups have been given the task of killing as many as possible of the technical staff of the station and of destroying as much as possible of the electronic apparatus, and everything that will burn must be burnt. Mines must be laid at the approaches to the building. All four groups can then depart in different directions.

The 'Shakespeare' group takes no part in the raid. Its task, beginning with the following night, is to lay the mines at the approaches to the building. Apart from that, with sniper fire and open attacks, the group has to make it difficult for anyone to attempt to save or restore the station. The group commander knows that the four neighbouring groups which are taking part in the attack are nearby and are doing the same. But the group commander does not know everything. He does not know that *spetsnaz* detachment 2-S-2, under the command of a major known as 'Uncle Kostya', has landed in the area of St David's. Detachment 2-S-2 consists of fifty-six men, fifteen lightweight motorcycles and six small cars with a considerable supply of ammunition. The detachment's task is to move rapidly, using secondary and forest roads and in some cases even the main roads, and reach the Forest of Dean to organise a base there. The Forest of Dean is a wonderful place for *spetsnaz* operations. It is a hilly area covered with dense forest. At one time it was an important industrial region. There are still the remains of the abandoned coal mines and quarries and railway tunnels, although it is a long time since there was any railway there. Once firmly established in that forest 'Uncle Kostya' can strike out in any direction: nearby there is a nuclear power station, the Severn bridge, a railway tunnel beneath the river Severn, the port of Bristol, the GCHQ government communications centre at Cheltenham, very important military factories also at Bristol and a huge munitions dump at Welford. The GRU believes that it is somewhere in this area that the Royal Family would be sent in the event of war, and that would be a very important target.

The four *spetsnaz* groups which have taken part at the outset in the operation against Brawdy depart immediately after the attack and make their different ways to the Forest of Dean where they can join up with Uncle Kostya's detachment. Shakespeare knows nothing about this. The large-scale raid on Brawdy and Shakespeare's continued activity in the following days and nights ought to give the enemy the impression that this is one of the main areas of operation for *spetsnaz*.

Meanwhile *spetsnaz* group 2-C-41, of twelve men, has been landed at night near the port of Felixstowe from the catamaran *Double Star*. The boat is sailing under the Spanish flag. The group has left the catamaran in the open sea and swum ashore with aqualungs. There it has been met by a *spetsnaz* agent recruited some years previously. He has at the GRU's expense bought a small motorcycle shop, and his shop has always had available at least fifteen Japanese motorcycles all ready for the road, along with several sets of leather jackets, trousers and crash helmets. The group (containing some of the best motorcyclists in the Soviet Union) changes its clothes, its weapons are wrapped in tarpaulin, the *spetsnaz* agent and his family are killed and their bodies hidden in the cellar of their house, and the motorcycle gang then rushes off at a great speed along the A45 in the direction of Mildenhall. Its task is to set up automatic Strela-Blok anti-aircraft missiles in the area of the base and knock out one of the most important American air bases in Europe, used regularly by F-111s. Afterwards the group is to make for the nearest forest and link up with *spetsnaz* detachment 2-C-5.

The group commander does not know that at the same time and not far away from him ten other *spetsnaz* groups, each working independently, are carrying out similar operations against the American military bases at Woodbridge, Bentwaters and Lakenheath.

■ ■ ■

The motor yacht *Maria* was built in Italy. In the course of a decade she has changed owners several times and visited the oceans of the world until she was sold to some wealthy person, after which she has not been seen for several years in any port in the world. But when the international situation takes a turn for the worse the *Maria* appears in the North Sea sailing under a Swedish flag. After some modernisation the appearance of the yacht has changed somewhat. On receiving the signal '393939' the *Maria* travels at full speed towards the coast of Great Britain. When it is inside British territorial waters and within range of Fylingdales Moor the yacht's crew removes hatch covers to reveal two BM–23 Katusha-like multi-barrelled missile-launchers. The sailors quickly aim the weapon at the gigantic spheres and fire. Seventy-two heavy shells explode around the installation, causing irreparable harm to the early warning system. The sailors on the yacht put on their aqualungs and jump overboard. For two hours the yacht drifts close to the shore without a crew. When the police clamber aboard, she explodes and sinks.

■ ■ ■

For operations against NATO forces in Central Europe the Soviet high command has concentrated an immensely powerful collection of forces consisting of the 1st and 2nd Western Fronts in East Germany, the 3rd Western Front in Poland, the Central Front in Czechoslovakia and the Group of Tank Armies in Belorussia. This makes fifteen armies altogether, including the six tank armies. On the right flank of this collection of forces there is the combined Baltic Fleet. And deep in Soviet territory another five fronts are being built up (fifteen armies altogether) for supporting attack.

On 12 August at 2300 hours *spetsnaz* battalions drawn from the seven armies of the first echelon cross the frontier of Western Germany on motorised hang-gliders, ordinary gliders and gliding parachutes. Operating in small groups, each battalion strikes at the enemy's radar installations, concentrating its efforts on a relatively narrow sector so as to create a sort of corridor for its planes to fly through. Apart from these seven corridors, another one of strategic importance is created. It was for this purpose that back in July the 13th *spetsnaz* brigade arrived in East Germany from the Moscow military district on the pretext that it was a military construction unit and based itself in the Thuringer Wald. The brigade is now split into sixty groups scattered about the forests of the Spessart and Odenwald hills, and faced with the task of destroying the anti-aircraft installations, especially the radar systems. In the first wave there are altogether 130 *spetsnaz* groups dropped with a total of some 3300 troops.

Two hours after the men have been dropped, the Soviet air force carries out a mass night raid on the enemy's anti-aircraft installations. The combined blow struck by the air force and *spetsnaz* makes it possible to clear one large and several smaller corridors through the anti-aircraft defence system. These corridors are used immediately for another mass air attack and a second drop of *spetsnaz* units.

Simultaneously, advance detachments of the seven armies cross the frontier and advance westwards.

At 0330 hours on 13 August the second wave of *spetsnaz* forces is dropped from Aeroflot aircraft operating at very low heights with heavy fighter cover.

The Central Front drops its *spetsnaz* brigade in the heavily wooded mountains near Freiburg. The brigade's job is to destroy the important American, West German and French headquarters, lines of communication, aircraft on the ground and anti-aircraft defences. This brigade is, so to speak, opening the gates into France, into which will soon burst several fronts and a further wave of *spetsnaz*.

The 1st and 2nd Western Fronts drop their *spetsnaz* brigades in Germany to the west of the Rhine. This part of West Germany is the furthest away from the dangerous eastern neighbour and consequently all the most vulnerable targets are concentrated there: headquarters, command posts, aerodromes, nuclear weapon stores, colossal reserves of military equipment, ammunition and fuel.

The *spetsnaz* brigade of the 1st Western Front is dropped in the Aachen area. Here there are several large forests where bases can be organised and a number of very tempting targets: bridges across the Rhine which would be used for bringing up reserves and supplying the NATO forces fighting to the east of the Rhine, the important air bases of Brüggen and Wildenrath, the residence of the German government and West Germany's civil service in Bonn, important headquarters near München-Gladbach, and the Geilenkirchen air base where the E–3A early-warning aircraft are based. It is in this area that the Soviet high command plans to bring into the battle the 20th Guards Army, which is to strike southwards down the west bank of the Rhine. The *spetsnaz* brigade is busy clearing the way for the columns of tanks which are soon to appear here.

The *spetsnaz* brigade of the 2nd Western Front has been dropped in the Kaiserslautern area with the task of neutralising the important air base and the air force command posts near Ramstein and Zweibrücken and of destroying the nuclear weapons stores at

Pirmasens. The place where the brigade has been dropped is where, according to the plan of the Soviet high command, the two arms of the gigantic pincer movement are to close together: the 20th Guards Army advancing from the north and the 8th Guards Tank Army striking from Czechoslovakia in the direction of Karlsruhe. After this the second strategic echelon will be brought into action to inflict a crushing defeat on France.

At the same time the Soviet high command understands that to win the war it has to prevent the large-scale transfer of American troops, arms and equipment to Western Europe. To solve the problem the huge Soviet Northern Fleet will have to be brought out into the Atlantic and be kept supplied there. The operations of the fleet will have to be backed up by the Air Force. But for the fleet to get out into the Atlantic it will have to pass through a long corridor between Norway and Greenland and Iceland. There the Soviet fleet will be exposed to constant observation and attack by air forces, small ships and submarines operating out of the fjords and by a huge collection of radio-electronic instruments and installations.

Norway, especially its southern part, is an exceptionally important area for the Soviet military leaders. They need to seize southern Norway and establish air and naval bases there in order to fight a battle for the Atlantic and therefore for Central Europe. The Soviet high command has allotted at least one entire front consisting of an airborne division, considerable naval forces and a brigade of *spetsnaz*. But airlifting ammunition, fuel, foodstuffs and reinforcements to the military, air and naval bases in Norway presents great problems of scale. So there have to be good and safe roads to the bases in southern Norway. Those roads lie in Sweden.

In the past Sweden was lucky: she always remained on the sidelines in a conflict. But at the end of the twentieth century the balance of the battlefield is changing. Sweden has become one of the most important strategic points in the world. If war breaks out the path of the aggressor will lie across Sweden. The occupation of Sweden is made easier by the fact that there are no nuclear weapons on its territory, so that the Soviet leaders risk very little. They know, however, that the Swedish soldier is a very serious opponent – thoughtful, disciplined, physically strong and tough, well armed, well acquainted with the territory he will have to fight over, and well trained for action in such terrain. The experience of the war against Finland teaches that in Scandinavia frontal attacks with tanks do not produce brilliant results. It requires the use of special tactics and special troops: *spetsnaz*.

And so it goes on, all over the world. In Sweden the capital city is reduced to a state of panic by the murder of several senior government figures and arson and bombing attacks on key buildings and ordinary civilians. In Japan, American nuclear bases are destroyed and chemical weapons used on the seat of government. In Pakistan, a breakaway movement in Baluchistan province, instantly recognised by the Soviet Communist Party, asks for and receives direct military intervention from the USSR to protect its fragile independence: Soviet-controlled territory extends all the way from Siberia through Afghanistan to the Indian Ocean.

It may not even need a third world war for the Soviet Union to occupy Baluchistan. The Red Army may be withdrawing from Afghanistan, but knowing what we know about Soviet strategy and the uses to which *spetsnaz* can be put, such a withdrawal can be seen as a useful public relations exercise without hindering the work of *spetsnaz* in any way. With a *spetsnaz* presence in Baluchistan, the Politburo could be reaching very close to the main oil artery of the world, to the Arab countries, to Eastern and Southern Africa, to Australia and South-east Asia: territories and oceans that are practically undefended.

THREAT ADVISORY July 30, 1987

This is an advisory from the Department of Energy's Office of Energy Emergencies.

The U.S. Government continues to believe that the risk of terrorist actions directed against U.S. diplomatic, military, and commercial facilities, as well as U.S. airline companies and merchant ships, has increased as a result of the reflagging of Kuwaiti tankers in the Persian Gulf. We have no, repeat no, specific information that a terrorist action is imminent. Statements made by pro-Iranian Groups and by Iranian leaders themselves suggest that targets within the United States as well as in the Persian Gulf, the Middle East, and Europe are being considered.

We urge you to maintain security awareness and will continue to advise you of this situation.

THREAT ADVISORY - September 8, 1987

This is an advisory from the Department of Energy's Office of Energy Emergencies.

There is no change from the advisory issued in late July, which stated:

> "The U.S. Government continues to believe that the risk of terrorist actions directed against U.S. diplomatic, military, and commercial facilities, as well as U.S. airline companies and merchant ships, has increased as a result of the reflagging of Kuwaiti tankers in the Persian Gulf. We have no, repeat no, specific information that a terrorist action is imminent. Statements made by Pro-Iranian Groups and by Iranian leaders themselves suggest that targets within the United States as well as in the Persian Gulf, the Middle East, and Europe are being considered."

We will continue to advise you on this situation. We anticipate contacting you again with another update as warranted.

THREAT ADVISORY - 10/20/87

This is an advisory from the Department of Energy's Office of Energy Emergencies.

"The U.S. Government believes that the recent U.S. retaliatory attack on an Iranian target in the Persian Gulf probably has increased the likelihood that Iran will engage in terrorist attacks against U.S. personnel and facilities. We have no, repeat, no specific information to indicate where such acts may occur, but American interests worldwide are judged to be at risk. Such attacks could occur with little or no additional preparation by Tehran."

The quoted text is a retransmission of one sent by the Department of State to overseas posts on 10/19/87, for distribution to U.S. industry contacts. Duplicate advisories may be received by companies with overseas affiliates which receive messages directly from the State Department through the Overseas Security Advisory Council.

We urge you to maintain security awareness and will continue to advise you on this situation. We anticipate contacting you again as developments require.

THREAT ADVISORY - 2/5/88

This is an advisory from the Department of Energy's Office of Energy Emergencies.

"Since mid-1987, the U.S. Government has issued a series of advisories concerning the possibility of Iranian-sponsored terrorist attacks against U.S. interests. The U.S. Government continues to believe that Iran remains capable of mounting such an attack with little or no warning. We further believe that the most probable venues for such action remain the Persian Gulf, elsewhere in the Middle East, or in Western Europe. We have no indication that Iranian policy vis-avis terrorism has changed, and that under certain circumstances they may choose this option."

The quoted text is a retransmission of one sent by the Department of State to overseas posts on 2/5/88, for distribution to U.S. industry contacts. Duplicate advisories may be received by companies with overseas affiliates which receive messages directly from the State Department through the Overseas Security Advisory Council.

We urge you to maintain security awareness and will continue to advise you on this situation. We anticipate contacting you again as developments require.

THREAT ADVISORY - 3/25/88

This is an advisory from the Department of Energy's Office of Energy Emergencies.

"The United States Government is not extending its previous threat advisory concerning possible anti-U.S. actions undertaken by or on behalf of the Iranian Government. A review of events of the past few months indicates that while prudent security measures should remain in effect, a formal threat advisory from the United States Government may no longer be appropriate."

The quoted text is a retransmission of one sent by the Department of State to overseas posts on 3/22/88, for distribution to U.S. industry contacts. Duplicate advisories may be received by companies with overseas affiliates which receive messages directly from the State Department through the Overseas Security Advisory Council.

This concludes the current threat advisory sequence. However, we urge you to maintain security awareness. We will be in contact with you should developments again require attention.

UNCLASSIFIED

THREAT ADVISORY - 4/18/88

This is an advisory from the Department of Energy's Office of Energy Emergencies.

"U.S. military action against certain Iranian targets on April 18 may result in increased risk to U.S. facilities and personnel from terrorist attack. We recommend increased security measures."

The quoted text is a retransmission of one sent by the Department of State to overseas posts on 4/18/88, for distribution to U.S. industry contacts. Duplicate advisories may be received by companies with overseas affiliates which receive messages directly from the State Department through the Overseas Security Advisory Council.

A separate event took place in New Jersey last week, when a suspected member of a Japanese terrorist group, carrying high explosives, was arrested. His mission/objectives remain unclear. In light of these developments we urge heightened security awareness.

UNCLASSIFIED

UNCLASSIFIED

THREAT ADVISORY - 4/27/88

This is an advisory from the Department of Energy's Office of Energy Emergencies.

"The U.S. Government possesses information which leads it to believe that the Government of Iran will authorize terrorist attacks against U.S. targets in the very near future. We further believe that these attacks will be deliberately designed to cause U.S. fatalities and/or destruction to U.S. facilities. We consider the Middle East, Southeast Asia, and Europe as the most likely areas for these attacks, although no area can be completely precluded as a possible area of operation. Security postures should be stringently reviewed, and additional measures taken if necessary."

The quoted text is a retransmission of one sent by the Department of State to overseas posts on 4/27/88, for distribution to U.S. industry contacts. Duplicate advisories may be received by companies with overseas affiliates which receive messages directly from the State Department through the Overseas Security Advisory Council.

We urge you to maintain security awareness and will continue to advise you on this situation. We anticipate contacting you again as developments require.

UNCLASSIFIED

ADVISORY

July 13, 1988

There have been numerous inquiries made to the Department of Energy (DOE) about the potential for a response to the airbus shootdown incident. The following message is being sent by the DOE's Office of Energy Emergencies in response to these queries.

The DOE has been in contact with appropriate government agencies concerning possible Iranian response to the downing of the airbus. The DOE has also reviewed current government traffic regarding this situation. At this time, there is no information regarding any threats directed toward U.S. energy facilities.

This message is similar to one sent recently by the Nuclear Regulatory Commission to companies and utilities involved with nuclear materials and power production. Therefore, some may receive both advisories.

Continued diligence in exercising security awareness plans is appropriate. The Department will continue to monitor the situation closely and will advise you as warranted.

American Petroleum Institute
1220 L Street, Northwest
Washington, D.C. 20005
202-682-8100

Charles J. DiBona
President

February 6, 1989

The Honorable
John Glenn
Chairman, Committee on Governmental Affairs
United States Senate
Washington, D. C. 20510

Dear Mr. Chairman:

The American Petroleum Institute (API) and the Association of Oil Pipe Lines (AOPL) wish to respond to your letter of January 24, 1989, concerning "the adequacy of government programs designed to prevent, or to respond to, major interruptions in telecommunications capabilities or energy supplies, whether caused by terrorist acts, sabotage, or natural disasters."

API is a national trade association representing over 200 companies engaged in all aspects of the petroleum industry. AOPL is an unincorporated association of 79 common carrier oil pipeline companies.

The nation's petroleum pipeline industry agrees with the Committee on Governmental Affairs that every reasonable measure should be taken to protect the security of the United States from disruptions of energy supply and vital telecommunications services. We are concerned, however, that our testimony at your Committee's public hearings on February 7 and 8 might have precisely the opposite effect from that intended. That is, by discussing specific points of possible vulnerability of the domestic petroleum pipeline system, we might be providing a roadmap for terrorism or sabotage. We would, however, be glad to provide the Committee with written comments or oral testimony if the Committee should hold closed hearings on this subject in the future.

The balance of this letter contains information that may be treated as written testimony. We hope that it will be helpful to the Committee as it considers adequacy of government programs in this area. We do ask that the information we provide in this letter be treated as confidential and shared only with Committee personnel on a need-to-know basis.

There are some 225,000 miles of petroleum pipelines in the United States. As a result of its physical size and corresponding geographical distance, the pipeline system is difficult to protect from a well-planned attack. At the same time, an effective assault on even a small percentage of these facilities would require many people and resources.

In its most fundamental sense, a pipeline is a tube between two geographic points. A break in this tube can cause disruption of service. With current technology and practices, most pipeline breaks can be repaired in a few hours. Disruptions of this type, which result most frequently from excavation damage, seldom cause a dislocation of supply, given the fast repair capability and elasticity of supply provided by routine storage at refinery and terminal distribution points.

Pipeline companies have security measures intended to impede trespassers and curtail vandals, as well as to prevent pipeline accidents and to monitor systems. Although these measures are not planned to deal directly with terrorist attacks, they do have some inhibiting impact. Surveillance of pipeline rights-of-way, either from the air or by walking along the pipeline, takes place at least every two weeks, primarily to check for encroachment or excavation activity. Also, of course, pipeline operating pressure is monitored continuously to alert the operator to any disruption in flow of product that might result from deliberate or natural causes.

Service disruptions could also be caused by problems at pumping stations, located at intervals along a petroleum pipeline to move the crude oil or refined products to their destination. Most pump stations depend on the public electrical grid system for power; the others are powered by diesel engines or gas turbines.

The elimination of a pump station typically would result in a slowdown, but only a marginal drop in throughput of the pipeline until the pump station was restored. The loss of the pump station, however, would not stop the operation of the pipeline, and in some pipeline systems excess pumping capacity would be able to absorb the loss entirely. Most pump stations, which may be manned or unmanned, are fenced, locked and lighted to discourage vandalism and unauthorized entry.

Critical parts generally are kept in supply by pipeline operators and are available for both ordinary maintenance and emergency situations. Nevertheless, similar pumps are used in pipelines all over the world. Emergency replacements could be obtained in short order through cooperative arrangements with other pipeline operators either in this country or elsewhere.

The tank farms are located at petroleum pipeline origination, breakout and termination points. Individual storage tanks are separated from one another by dikes to contain and localize any fire or spillage from the tanks. It would be difficult, although not impossible, for an explosion or fire by sabotage or terrorist act to consume an entire assemblage of tanks since the spacing of diking of tanks is to isolate a burning or leaking tank from others. A separate act of terrorism or sabotage likely would result in the destruction of only a portion of the tankage, in which case there would be a comparatively less disruptive effect on operations.

The last significant petroleum pipeline location that warrants discussion is the control room, from which the pipeline is operated remotely by means of computers and telecommunications circuits connected to the valves, pump stations and sensors along the pipeline. Access to petroleum pipeline control rooms is limited to employees and management-approved visitors, and the rooms themselves are locked at all times. If a control room were destroyed, the functions it provides could be performed in some instances by a backup facility, or by satellite control centers along segments of the pipeline. In the last resort, control functions could be performed manually, as indeed they were before the technological developments that made possible today's automated operations. We are confident that in an emergency U.S. companies would provide, on an immediate basis, any additional skilled manpower needed in a serious emergency.

In all of the above situations it should be borne in mind that interrupted shipments through a temporarily disabled pipeline could be offset by shipments through other pipelines serving the same markets, shipments via alternative modes of transportation, and or through product supply available from refineries and terminals in the same region.

As noted, U.S. petroleum pipeline operators currently provide security to prevent vandalism, theft and other damage to their facilities by ordinary criminals. To date, pipeline operators have kept such damage at a minimum. Ultimately, the industry depends upon the U.S. government, and its armed services and intelligence agencies, to protect its facilities from domestic or foreign conspirators with sufficient resources and sophistication to mount a serious attack on the nation's pipeline system.

We are enclosing three final draft copies of Volume V, Petroleum Liquids Transportation, of a study by the National Petroleum Council, Petroleum Storage & Transportation. The study examines the U.S. petroleum industry and its susceptibility to supply disruptions. We believe that your Committee will find the report useful as you assess current levels of security. These reports are not confidential.

Your letter asked for suggestions on how the U.S. government could improve its measures to prevent or mitigate sabotage or terrorist activity. Petroleum pipeline operators have had consistently positive and cooperative assistance from the Federal Bureau of Investigation in maintaining protection over their facilities. Nevertheless, the recent experience with a terrorist bombing of a U.S. airplane in Scotland suggests that additional communication is needed between the U.S. government and commercial operators of facilities.

In closing, we emphasize our willingness to cooperate fully with your Committee in its investigation. We would be pleased to discuss these matters further with you, other members of the Committee, and Committee staff. If you have any additional questions about this matter, please feel free to contact Tom Farley of my staff at 682-8416.

Sincerely,

Charles J. DiBona

Attachments (3)

Report of The Interagency Group on Energy Vulnerability

November 1986 - November 1988

January 1989

Prepared for the
Senior Interagency Group
for
National Security Emergency Preparedness

TABLE OF CONTENTS

Introduction... 1

Subgroup Reports

Energy Vulnerability Assessment Subgroup............. 11
Database and Projections Subgroup.................... 15
Response Development Subgroup........................ 18

Appendices

A. Interagency Group on Energy Vulnerability Charter and Concept Paper.................................... 23
B. Energy Vulnerability Assessment Subgroup Charter..... 26
C. Database and Projections Subgroup Charter............ 28
D. Response Development Subgroup Charter................ 31

List of Acronyms... 34

REPORT
of
THE INTERAGENCY GROUP ON ENERGY VULNERABILITY
November 1986 - November 1988

Introduction

The United States is dependent on energy to carry out numerous tasks. Everyone is affected. From lighting our homes, to fueling our transportation systems, to providing fuel for our military aircraft, energy supply is a critical factor. Pipelines, electric utility lines, and supertankers constitute some of the ways in which our energy reaches us. These domestic and international supply systems are vulnerable to disruptions from embargoes, sabotage, terrorism, or natural disasters. All energy system components, including generation and production, need to be examined and monitored to ascertain their potential vulnerabilities. The next logical step would be to reduce these recognized vulnerabilities through Government/industry efforts. We must assure that the Nation, at all times, has sufficient energy to meet defense and other vital needs.

President Reagan's energy policy is strongly committed to ensuring an adequate, reasonably priced energy supply for the United States.

Thus, on September 16, 1985, the President approved and signed National Security Decision Directive 188 (NSDD-188) on Government Coordination for National Security Emergency Preparednesss (NSEP). This Directive provided the framework for the Senior Interagency Group for National Security Emergency Preparedness (SIG-NSEP) and the development of initiatives to reduce identified vulnerabilities of threats to energy systems.

On April 11, 1986, the SIG-NSEP authorized the creation of the Interagency Group on Energy Vulnerability (IG-EV). Responsibility for its establishment and for the designation of a chairman was given to the Secretary of the Department of Energy (DOE), John S. Herrington.

The IG-EV's department and agency membership was determined and approved by the SIG-NSEP and on October 3, 1986, Secretary Herrington corresponded with the various Secretaries and Heads of those agencies. He requested their support and the designation of a representative with national security emergency preparedness responsibilities. The IG-EV was subsequently formed, and the first meeting was held November 13, 1986.

PURPOSE

The IG-EV was organized to address the most effective means of responding to threats against U.S. energy systems (e.g., oil, natural gas, electricity, or coal). It focuses on national policy relating to U.S. energy system vulnerabilities. It also develops initiatives to decrease this vulnerability and to mitigate the impact any disruptions might have on national security.

As required by the IG-EV's Charter (see Appendix A, page 23), subgroup recommendations are reviewed, approved, and coordinated through the IG-EV, with conclusions and recommendations submitted to the SIG-NSEP for approval. The IG-EV reports to the SIG-NSEP through the Director of Defense Policy, of the National Security Council staff.

The IG-EV is a policymaking body. Supporting staff actions, issues, and projects are assigned to the IG-EV's three subgroups (Energy Vulnerability Assessment, Database and Projections, and Response Development) through, and with the guidance of, the IG-EV. These tasks are carried out by the responsible Subgroup and reports are provided to the IG-EV, which has oversight responsibilities. A key component of each IG-EV meeting is reports by the Subgroup chairmen on their respective group's activities.

BACKGROUND

The IG-EV is comprised of Assistant Secretary-level representatives from the various agencies and departments having a major role in national energy vulnerability issues. As shown in Figure 1, 15 Federal agencies and departments are represented.

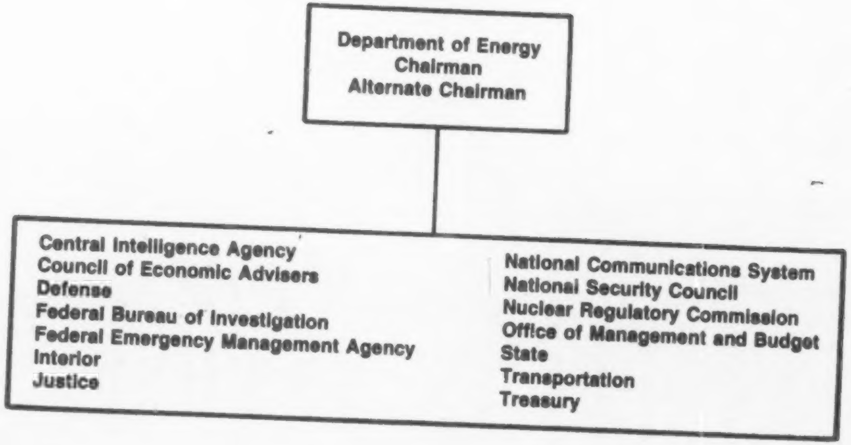
David B. Waller, Assistant Secretary for International Affairs and Energy Emergencies, DOE, was designated to chair the Group. Edward V. Badolato, Deputy Assistant Secretary for Energy Emergencies, DOE, serves as his alternate.

To date, the IG-EV has met nine times, once each quarter, beginning with an initial organizational meeting in November 1986. Briefings on the background of NSDD-188 were held at this first meeting, and a Charter and Concept Paper on

Figure 1

Interagency Group on Energy Vulnerability

Membership



Department of Energy
Chairman
Alternate Chairman

Central Intelligence Agency
Council of Economic Advisers
Defense
Federal Bureau of Investigation
Federal Emergency Management Agency
Interior
Justice

National Communications System
National Security Council
Nuclear Regulatory Commission
Office of Management and Budget
State
Transportation
Treasury

the IG-EV's mission and organization (see Appendix A, page 23) were considered and approved. It was determined at this meeting that the work of the IG-EV would be conducted principally in three working groups, outlined in Figure 2. It was further noted that each Subgroup chairman has responsibility for developing and recommending to the IG-EV for approval the specific focus and milestones for his respective subgroup.

During the past two years, the IG-EV has been organized with its three working level Subgroups. Each subgroup's major responsibilities are:

- Energy Vulnerability Assessment Subgroup

  Co-chaired by DOE and the Department of Defense, this Subgroup was tasked with examining the U.S. energy systems' vulnerability to non-routine disruptions which may impact on national security.

- Database and Projections Subgroup

  Chaired by DOE, the Database Subgroup has the responsibility of analyzing the impacts of the changing marketplace on energy systems and of continuing to develop an information base for assessing potential impacts of energy supply interruptions.

- Response Development Subgroup

  Co-chaired by DOE and the State Department, this Subgroup has the responsibility of evaluating response measures and international activities which could conceivably be implemented should an energy emergency arise.

More comprehensive reports of the Subgroups' activities are contained in the body of this report.

ENERGY ISSUES

The Group has served well as a forum for timely presentations addressing energy vulnerability issues.

As illustrated in Figure 3, the IG-EV has been briefed on numerous substantive energy issues over the past two years.

Figure 2

Interagency Group
on Energy Vulnerability

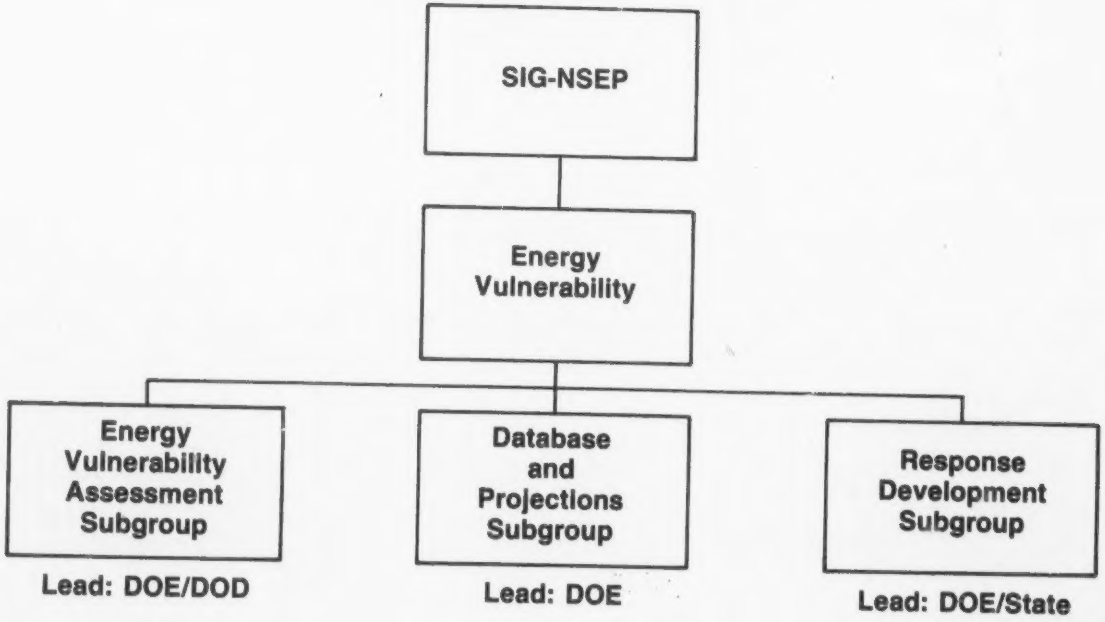

SIG-NSEP
Energy Vulnerability
Energy Vulnerability Assessment Subgroup
Lead: DOE/DOD
Database and Projections Subgroup
Lead: DOE
Response Development Subgroup
Lead: DOE/State

Figure 3

PRESENTATIONS

1986

PRESENTATION	PRESENTER
NSDD-188 Review	Ronald St. Martin National Security Council
IG-EV Overview	Edward V. Badolato Alternate IG-EV Chairman Department of Energy
Strategic Petroleum Reserve Size Study	John Stanley-Miller Policy, Planning and Evaluation Department of Energy
National Electric Reliability Council Initiative	Glenn Coplon Energy Vulnerability Assessment Subgroup Department of Energy
1987	
Energy Security Study Review	William F. Martin Deputy Secretary Department of Energy
Energy Security Study Update	Margaret W. Sibley Director of Policy Integration Policy, Planning and Analysis Department of Energy

1987 (Continued)

PRESENTATION	PRESENTER
"An Energy Evaluation" (Blue Book)	W. David Montgomery Director, Office of Energy Markets and End Use Energy Information Administration Department of Energy
International Energy Agency Ministerial Meeting Overview, May 11-May 12, 1987	David B. Waller IG-EV Chairman Department of Energy
Middle East Developments	Wendell Coote Central Intelligence Agency
Wintex-Cimex Exercise Update	Romulo L. Diaz, Jr. Response Development Subgroup Department of Energy
Defense Industry Readiness Conditions	Craig Alderman, Jr. Deputy Under Secretary for Policy Department of Defense
Global Wargame '87	Dr. Thomas Etzold Staff Consultant Department of Energy
Energy Aspects of the Industrial Base Initiative	Edward V. Badolato Alternate IG-EV Chairman Department of Energy
Energy Emergency Management System/Strategic Petroleum Reserve Exercise (EEMS/SPR)	Finn Neilsen Co-Chairman Response Development Subgroup Department of Energy

1988

PRESENTATION	PRESENTER
Strategic Petroleum Reserve Drawdown Capabilities	Richard D. Furiga Deputy Assistant Secretary for Petroleum Reserves Fossil Energy Department of Energy
San Francisco Simulation of Regional Energy Vulnerabilities	Edward V. Badolato Alternate IG-EV Chairman Department of Energy
Coordinated Emergency Response Measures Test (CERM)	Finn K. Neilsen Co-Chairman Response Development Subgroup Department of Energy
New Energy Technologies and Their Impact on Long-Term Energy Vulnerability	
- Enhanced Oil Recovery	George Stosur Fossil Energy Department of Energy
- Clean Coal Technology	Dr. Larry M. Joseph Fossil Energy Department of Energy
- Alternative Transportation Fuels	Dr. Carmen DiFiglio Policy, Planning and Analysis Department of Energy

1988 (Continued)

PRESENTATION	PRESENTER
Sixth Allocation Systems Test (AST-6)	Romulo L. Diaz, Jr. Response Development Subgroup Department of Energy
Federal Bureau of Investigation's Counter-Terrorism Approach to Infrastructure Matters	Bob A. Ricks Deputy Assistant Director Criminal Investigative Division Federal Bureau of Investigation
Report on AST-6	Romulo L. Diaz, Jr. Response Development Subgroup Department of Energy
Global Wargame '88	Edward V. Badolato Alternate IG-EV Chairman Department of Energy
An Overview of EPA's Regulations For Underground Storage Tank Systems and the Underground Fuel Storage Problems in the Communications Industry	Edward V. Badolato Alternate IG-EV Chairman Department of Energy and Capt. Karen L. Manos Defense Communications Agency

The IG-EV has served as a platform for considering new ideas as well as for considering important energy issues. It has brought senior Administration officials together in order to deal with pre-crisis management issues. Further, this Group would be convened during an energy crisis for the coordination of Federal responses. It was tested during two 1988 International Energy Agency (IEA) tests, the Coordinated Emergency Response Measures (CERM) test and the Sixth Allocation Systems (AST-6) test.

SUMMARY

Secretary of Energy John Herrington clearly stated the President's commitment for a secure energy industry, when he stated in the Department of Energy's Energy Security Study:

> "Energy security considerations carry tremendous weight and are cause for deep concern for every American. We cannot afford to be complacent. Energy security is a vital part of the foundation on which our foreign and domestic policies--and our economy--rest. As a Nation, we must recognize the warning signs and take thoughtful and prudent action that meets our responsibility to consumers, industry, and the Nation alike."

The Interagency Group on Energy Vulnerability is fully committed to continuing its support of an energy-secure Nation.

The following sections of this report to the SIG-NSEP highlight the IG-EV's cumulative accomplishments, as performed by its three Subgroups, over the past two years.

ENERGY VULNERABILITY ASSESSMENT SUBGROUP

The Energy Vulnerability Assessment Subgroup (EVAS) was formed by the IG-EV in November 1986. It is co-chaired by the Department of Energy and the Department of Defense. Its charter (see Appendix B, page 26) was developed by the EVAS at its February 6, 1987, meeting and approved by the IG-EV on February 25, 1987.

PURPOSE

The EVAS was created to examine the vulnerability of U.S. energy systems to non-routine disruptions that may affect national security. It proposes actions which could be implemented in advance to reduce the likelihood or impact of disruptions by increasing the level of emergency preparedness. Energy systems of interest include electric power, crude oil and petroleum products (imports, production, refining, distribution), natural gas, and coal.

BACKGROUND

The EVAS is made up of 15 Federal departments and agencies. The Subgroup is co-chaired by Robert M. Guth, Director of Energy Emergency Operations in the Department of Energy, and by Jeffrey Jones, Director of Energy Policy in the Office of the Secretary of Defense.

ACCOMPLISHMENTS

San Francisco Energy Emergency Simulation

To explore the readiness of crisis management plans and procedures intended for use in the event of an energy disruption, the EVAS held an Energy Emergency Simulation in San Francisco, California on December 16-18, 1987. The 73 attending participants represented a broad spectrum from local energy supply firms, defense users, and state and Federal emergency agencies. The types of energy considered were petroleum products, natural gas, and electric power.

The objectives of the Simulation were to:

(1) Identify categories of essential defense and public services end-users of energy in the San Francisco Bay area;

(2) Assess the ability of crisis management mechanisms already in place to ensure needed energy supplies to essential end-users;

(3) Assess whether the San Francisco analysis process would be useful for studying energy vulnerabilities in other key areas of the Nation; and,

(4) Sensitize Federal, state, and industry representatives to the possibility and impact of non-routine energy supply disruptions (e.g., resulting from mobilization or sabotage).

The major conclusions of the Simulation were:

(1) The participants could identify some, but not all, categories of essential end-users in the area;

(2) Existing Federal and state crisis management plans are not well coordinated and may be at cross purposes;

(3) The San Francisco analysis process is transferable to other regions. However, energy supply infrastructure and end-use dissimilarities are expected to make each region unique; and,

(4) The participants gained valuable insights into the potential problems caused by disruptions and the national interest questions involved. Utilities (electric and gas) were reluctant to identify specific facilities which, if sabotaged, would result in major disruptions.

National Security Emergency Preparedness (NSEP) Energy Program

An NSEP energy program, under EVAS auspices, is currently underway. Its goal is to reduce the impact or likelihood of energy disruptions on end-users whose continued operation is deemed essential to national security. The program consists of two tracks, A and B.

Track A focuses on the near-term need for crisis management plans to minimize the impact of disruptions in the supply of energy to essential end-users. Under Track A, EVAS member agencies are identifying essential Federal functions under various disruption scenarios. These functions will be identified to state and local governments and energy firms for subsequent improved coordination of Federal, state, and industry crisis management plans.

Track B focuses on longer-term actions to reduce excessive vulnerabilities of the energy supply infrastructure to disruptions which may affect national security. Under Track B, a methodology is under development to identify excessive vulnerabilities and mitigating options. It is planned that this methodology will be applied initially in areas with the highest concentrations of national security related end-users. This methodology will first be applied to a pilot study area and, following verification, will be considered for expansion to national application.

National Security Telecommunications/Energy Projects

The National Communications System has been charged to ensure that a responsive and survivable national telecommunications infrastructure is developed to meet NSEP needs. To help address this concern, the President requested the telecommunications industry to form the National Security Telecommunications Advisory Committee (NSTAC). The EVAS has worked closely with the NSTAC's Telecommunications System Survivability Task Force and, subsequently, its Energy Task Force.

The Subgroup undertook several telecommunications-related projects:

(1) Identifying mutual interdependencies between energy and telecommunications;

(2) Identifying essential energy needs for telecommunications services;

(3) Identifying essential telecommunications needs for energy supplies;

(4) Identifying telecommunications restoration priorities needed by energy supply systems following disruptions occurring under peacetime (business as usual), crisis/mobilization, conventional war, or nuclear war conditions; and

(5) Design of a joint simulation involving a service disruption to both industries and the coordinated response likely to be needed.

Information Exchange

The EVAS meetings include information exchanges on a wide variety of topics of interest to the member agencies. During the last two years, such topics included reports on energy-related simulations conducted by the Department of Energy and other agencies. Other discussion topics included the impact of the drought on energy supplies and programs by energy suppliers to reduce the vulnerability of their facilities to sabotage and terrorism.

CONCLUSION

Since its formation two years ago, the EVAS has identified the aspects of existing Federal, state, and energy industry crisis management plans needing improved coordination and is working to achieve the necessary improvements.

Reducing excessive vulnerabilities of the energy supply infrastructure is inherently a longer term and complex project. The analytic methodology for vulnerability identification will be tested by the end of 1988. Work planned for 1989 includes achieving an interagency consensus on the definition of threats for analytic purposes, working with industry to identify vulnerability mitigating options and costs, and expanding the program nationally. Work has begun on identifying energy and telecommunications industry mutual dependencies and developing coordinated crisis management plans.

Database and Projections Subgroup

Pursuant to NSDD 188 and by the direction of the Interagency Group on Energy Vulnerability, the Database and Projections Subgroup (DPS) was formed in November 1986. The Subgroup is chaired by the Department of Energy. Its charter (see Appendix C, page 28) was developed by the DPS at its January 27, 1987, organizational meeting and approved by the IG-EV on February 25, 1987.

PURPOSE

The objective of the Database and Projections Subgroup is to provide the information base and analytical capabilities for assessment of energy security issues.

BACKGROUND

The DPS has an active membership from 14 Government departments and agencies. W. David Montgomery, Director of the Energy Information Administration's Office of Energy Markets and End Use, DOE, chaired the DPS until March 25, 1988. W. Cal Kilgore was then named Director of that office and assumed the DPS chairmanship.

The Subgroup provides an excellent forum for the exchange of analytical ideas related to the area of energy vulnerability. The Subgroup provides for a monthly exchange of energy information between agencies and meets four times a year to develop consensus quarterly world oil outlooks. These Subgroup activities ensure that all of the Government agencies dealing with energy vulnerability matters are sharing and discussing the same energy outlook.

ACCOMPLISHMENTS

An Energy Evaluation (Blue Book)

The major ongoing responsibility of the Subgroup is the classified semi-annual report, An Energy Evaluation (Blue Book), which presents a current assessment of United States and allied vulnerability to oil supply disruptions. The Blue Book provides all policymakers with the same baseline data and forecasts on the world oil market and an assessment of U.S. vulnerability to a range of possible disruptions in oil supplies from the Middle East.

The oil market projections are updated by the Subgroup quarterly so that the latest quarter is always available to examine, in case a real disruption occurs. However, the supply disruption analysis is updated semiannually, with issue or information papers updated and developed as necessary. Since the IG-EV was established and the DPS assumed the responsibility for the Blue Book from its predecessor group, four Blue Books and four interim oil market outlooks have been developed and transmitted to relevant policymakers within the Government.

During this time, the Subgroup has also requested and received a new evaluation by the intelligence community (Interagency Damage Assessment Team/IDAT) of the most probable oil supply disruptions that should be evaluated in the Blue Book.

With each Blue Book the Subgroup performs several related activities. In addition to updating accompanying issue/information papers (such as a Middle East pipeline paper), Stand-by Public Affairs Information Packets on the Persian Gulf are also periodically revised.

These Stand-by Information Packets are unclassified and are available for immediate public use along with the Subgroup's most current outlook of the impacts of a supply disruption.

Accompanying each Blue Book is a classified Situation Analysis Report. In May 1987, a special Situation Analysis Report from the Second Quarter 1987 Blue Book was prepared as a briefing package for the Deputy Secretary of Energy's use before the Senate Energy Committee.

The personal computer model, the Disruption Impact Simulator (DIS), used to develop the analysis in the Blue Book has been refined with an improved methodology for estimating economic impacts. The updated DIS information is provided to the Office of International Affairs and Energy Emergencies every quarter for use in its Decision Support System. The Subgroup chairman has also provided demonstrations and briefings on the DIS model to the IEA, various state energy offices, industry, congressional staffs, and to the Department of Energy's Secretary, Deputy Secretary, and Under Secretary.

The analysis techniques developed by the Subgroup have had far-reaching uses, possibly more than originally planned for in the Subgroup's Charter. For example, the analysis methodology in the DIS has been used as the basis for U.S. participation and analysis in several interagency and international/intergovernmental emergency tests and exercises. The Subgroup's estimates and analysis were used in the North Atlantic Treaty Organization's (NATO) and the IEA's emergency tests.

The Blue Book was also used to meet the requirements of the National Defense Authorization Act. A very specific study on the Persian Gulf was mandated in that Act and the Blue Book analysis and forecasts were utilized. The chairman of the Subgroup, along with the Department of Defense and Central Intelligence Agency Subgroup members, also briefed the Senate Energy and Natural Resources Committee staff on the current Blue Book and IDAT disruption scenarios and provided a demonstration of the DIS model.

Fact Sheets

The Subgroup has also developed Fact Sheets, as the need arises (i.e., Iranian/Iraqi Import Fact Sheets), for distribution throughout the Government. Once again, these unclassified Fact Sheets (often updated monthly or quarterly) provide all parts of the Government with the same unclassified information to answer public inquiries such as questions pertaining to the Persian Gulf.

Global Computer-Based Mapping System

The Subgroup was also tasked by the IG-EV to develop a survey of global computer-based mapping systems. The survey presented information on current computer-based mapping efforts within the Federal Government and the private sector. When the IG-EV acquires a system, the Subgroup could develop a geographically based database of energy production and distribution facilities. A computer-based mapping system, with an energy infrastructure database, could provide the IG-EV with a valuable tool for planning and evaluating impacts on energy facilities during emergency situations.

CONCLUSION

As real world events (such as the events during 1988 in Panama) have taken place over the last two years, the DPS support staff has always been involved, providing briefings to DOE's Energy Emergency Management Team.

By providing Blue Books, Standby Public Information Packets, Situation Analysis Reports, and Fact Sheets to a large group of policymakers, the DPS clearly meets its objective of establishing an information base and analytical capabilities for assessment of energy security issues.

RESPONSE DEVELOPMENT SUBGROUP

At its November 13, 1986, initial meeting, the Interagency Group on Energy Vulnerability authorized the establishment of the Response Development Subgroup (RDS), co-chaired by the Department of Energy and the Department of State. The RDS charter (see Appendix D, page 31) was developed by the RDS at its first meeting held on January 29, 1987, and approved by the IG-EV on February 25, 1987.

PURPOSE

The RDS was organized to consider the implications of disruptions to U.S. energy systems and to develop policy options that would mitigate any adverse impacts on the domestic economy. Any policy measures developed by the RDS are to be forwarded to the Interagency Group on Energy Vulnerability for review and consideration.

BACKGROUND

The RDS is comprised of 16 Federal departments and agencies that could be involved with developing or implementing major Federal response actions during an energy emergency. The IG-EV members selected knowledgeable senior officials with authority to act on behalf of their department or agency to serve as members of the Response Development Subgroup. Also, Subgroup membership includes interested Federal departments or agencies not designated as members of the IG-EV.

Finn Neilsen, Director of the Office of Energy Emergency Plans and Integration, has served as the DOE co-chairman of the Subgroup. Because of the international nature of possible energy supply disruptions and potential responses that could be contemplated in an energy emergency, the Department of State also co-chairs the Subgroup. Daniel Serwer, Director of the Office of Energy Consumer Affairs, served as the initial co-chair until September 1987. Ann Hollick replaced Mr. Serwer for one year and, on September 2, 1988, Stuart Allan became the RDS co-chairman representing the Department of State.

ACCOMPLISHMENTS

Global Energy Security

The focus of the RDS has been on interagency planning and execution of U.S. responses to major supply interruptions, including interagency coordination. RDS members have been regularly briefed on world events that could impact the security of U.S. energy systems.

At the April 1987 RDS meeting, Deputy Assistant Secretary for Energy Emergencies, Mr. Badolato, provided an overview of the high level review of DOE's landmark report on Energy Security. This report, from the Secretary of Energy to the President, found that a growing reliance on imported oil, especially from the Persian Gulf region, could have serious implications for national security. Later, Col. Kiely, United States Marine Corps, Political Military Bureau of the State Department, discussed the ongoing Persian Gulf situation and the build-up of U.S. Forces.

At the July 1987 meeting, Col. Dick Gannon (retired), United States Marine Corps, Anti-Terrorism Assistance Division, Department of State, told the Subgroup about efforts to develop and enhance anti-terrorism efforts of friendly foreign governments which would improve the security of foreign oil-producing states.

In November, Mr. Badolato reported on his month-long, 8-nation trip through the Middle East with Secretary of Energy John S. Herrington and Assistant Secretary for International Affairs and Energy Emergencies, David B. Waller. Secretary Herrington brought the message to the Gulf that the United States will ensure that trade will continue through the open trade routes of the Persian Gulf and that the United States is willing to expand dialogue with the Gulf States on energy matters.

These briefings have heightened the insight of the Subgroup to the major issues of the world oil situation.

International Energy Agency (IEA)

An important element of DOE's emergency response program is the continuing commitment by the United States to the International Energy Agency to assure mutual preparedness in the event of a major petroleum supply disruption.

During 1988, the RDS was activated during two IEA tests to test U.S. interagency procedures for implementing an early response to international oil supply disruptions: the Coordinated Emergency Response Measures (CERM) test in January-February and the Sixth Allocation Systems Test (AST-6) in September-November. Thus, for the first time, an interagency process has been used to coordinate U.S. responses to an international energy emergency. The simulation of the IG-EV by the RDS proved to be very useful in coordinating plans and implementing U.S. policy involving energy disruptions.

In both tests the hypothetical disruption was evaluated, a formal Situation Analysis Report was developed, and a Response Options Paper was prepared for a simulated Presidential decision. By simulating the IG-EV process, the Department of Energy tested the lead agency concept and proved the value of the IG-EV process by developing the proposed U.S. position with other Federal departments and agencies.

Additionally, in April 1987, the IEA sponsored a workshop on oil demand restraint as an emergency response measure. As an alternative, the U.S. position emphasized that releasing strategic petroleum stocks, such as the U.S. Strategic Petroleum Reserve (SPR), would be the most effective means of limiting economic damage resulting from an oil disruption. The United States also addressed the problems associated with the implementation of demand restraint programs, based on U.S. experience. These positions were coordinated with other Federal departments and agencies through the April 7, 1987, RDS meeting. The early release of the SPR has been a consistent Administration policy for dealing with an international petroleum supply disruption.

North Atlantic Treaty Organization (NATO)

One of the top priorities of NATO's Petroleum Planning Committee (PPC) is civil petroleum planning activities to ensure that essential civil and military defense needs are met during crisis and war. Through the RDS, Federal departments and agencies were briefed on DOE's responsibilities in NATO civil emergency planning for petroleum. For example, the current PPC effort regarding the implications of implementing the single fuel concept was discussed. This coordination process was useful in developing U.S. positions for presentation to the PPC.

In addition, the Subgroup was updated on the high state of readiness of the NATO Wartime Oil Organization (NWOO) and the 1988 NWOO Training Session held in Iceland. The session's purpose was to train Government and industry personnel regarding organization, mission, and communications. Within the Western branch of the NWOO, headquartered in the United States, DOE chairs the executive body, represents the U.S. Government, and performs essential Secretariat functions. It was concluded that similar briefings on DOE's NATO activities would serve to keep the Subgroup abreast of current and future DOE initiatives in the NATO area.

Response Development Subgroup Communications Directory

The RDS Secretariat maintains a current list of Subgroup members and alternate members containing their addresses, telephone, telefax and telex numbers within their agencies, and their current levels of security clearance. This Directory has proven useful for quick coordination of simulated interagency responses in recent tests, and would be used during an actual energy emergency.

Conclusion

During the past two years, the RDS has been evaluating and improving interagency processes for responding to possible disruptions of U.S. energy supply systems. Procedures have been developed and reviewed to ensure that in advance of an energy emergency, there is interagency consensus on appropriate response policies. These activities have focused on petroleum supply disruptions initially, with expansion to other U.S. supply systems contemplated in future RDS activities.

Appendix A

CHARTER OF THE
INTERAGENCY GROUP ON ENERGY VULNERABILITY
OF THE
SENIOR INTERAGENCY GROUP
FOR
NATIONAL SECURITY EMERGENCY PREPAREDNESS

Pursuant to National Security Decision Directive (NSDD) Number 188, "Government Coordination for National Security Emergency Preparedness," and by direction of the Senior Interagency Group for National Security Emergency Preparedness (SIG-NSEP), the Interagency Group on Energy Vulnerability (IG-EV) is hereby established.

Objective:

To develop policy recommendations that would seek to assure adequate energy security at reasonable cost.

Purpose:

The purpose of the IG-EV is to focus on national policy issues relating to the vulnerability of U.S. energy systems, and develop policy options to reduce this vulnerability. The IG-EV will examine the vulnerability of U.S. energy systems to disruptions and develop initiatives both to decrease this vulnerability and to mitigate the impact on national security of any disruptions; it will also address the anticipated capacity or inadequacy of these systems to meet national security needs.

Scope:

The IG-EV will review potential vulnerability to U.S. energy systems, which include: electric power, crude oil and petroleum products (imports, production, refining, distribution), natural gas, and coal.

Procedure:

Selected and assigned studies and evaluations will be conducted by the IG-EV through working level subgroups to which it will assign issues and provide guidance. Recommendations by the subgroups will be reviewed, approved, and coordinated by the IG-EV which will pass appropriate conclusions and recommendations to the SIG-NSEP.

Subgroups will address issues within their purview and prepare option papers reflecting agency views. Members of the IG-EV are invited to participate in each of the subgroups.

Membership:

Membership of the IG-EV is composed of senior representatives with national security emergency preparedness responsibilities from the following departments and agencies:

Chaired by:	Department of Energy
Member Departments/ Agencies	Department of Defense Department of Justice Department of the Interior Department of State Department of Transportation Department of the Treasury Central Intelligence Agency Federal Bureau of Investigation Federal Emergency Management Agency National Communications System National Security Council Nuclear Regulatory Commission

Additional members may be added to the IG-EV as needed

Subgroups:

Each subgroup will be comprised of knowledgeable department or agency officials with authority to act on behalf of their department or agency. Subgroup membership may include, as necessary, departments or agencies not designated as members of the IG-EV. Subgroups of the IG-EV and their chairs are as follows:

- Energy Vulnerability Assessment Subgroup - DOE/DOD co-lead
- Database and Projections Subgroup - DOE/EIA lead
- Response Development Subgroup - State/DOE co-lead

Other subgroups may be formed as determined by the IG-EV.

Appendix A

INTERAGENCY GROUP ON ENERGY VULNERABILITY
CONCEPT PAPER

The mission of the Interagency Group on Energy Vulnerability (IG-EV) is to examine the vulnerability of U.S. energy systems, and to propose options to reduce this vulnerability or to mitigate the impacts of a disruption of energy systems. Energy vulnerability refers to the susceptibility of U.S. energy supplies to nonroutine disturbances which may affect national security. Such systems include domestic production and delivery systems and imports.

Disruption of any type of energy (i.e., oil, natural gas, electricity, or coal) may affect national security. For example, with the recent decline in oil prices, our dependency on importd oil is expected to increase substantially, increasing the risk to national security from an oil disruption. As an example of another type of energy, electricity supplies for vital defense industries may be vulnerable to terrorist or sabotage attacks. The impacts of such attacks could be exacerbated by the lack of critical spare parts, as well as the lack of alternative generation or transmission capabilities.

National security requirements for energy must be determined jointly with other Federal agencies. Therefore, the examination of energy vulnerability and development of initiatives require interagency coordination and action. NSDD-188 provides the framework to address such matters through the IG-EV and, ultimately, the SIG-NSEP.

The work of the IG-EV will be conducted principally in working level subgroups. Three subgroups are proposed initially: the Energy Vulnerability Assessment Subgroup, the Database and Projections Subgroup, and the Response Development Subgroup.

The Energy Vulnerability Assessment Subgroup will identify the vulnerability of energy systems to disruptions of all types and to anticipated inadequate capacity. DOE and DOD will co-chair this group.

The Database and Projections Subgroup will continue to develop an information base for assessing the potential impacts of energy supply interruptions. DOE/EIA will lead this group. Since 1983, an interagency working group has periodically assessed the vulnerability of the United States to a disruption in oil supplies from the Middle East. This assessment will be expanded to cover other fuels, as appropriate.

The Response Development Subgroup will develop and insure implementation of initiatives to mitigate the impact of energy disruptions or threats on national security. State and DOE will co-chair this group, with State focusing on international aspects and DOE focusing on domestic aspects.

Appendix B

CHARTER OF THE ENERGY VULNERABILITY ASSESSMENT SUBGROUP OF THE INTERAGENCY GROUP ON ENERGY VULNERABILITY

Pursuant to National Security Decision Directive (NSDD) Number 188 and by direction of the Interagency Group on Energy Vulnerability (IG-EV), the Energy Vulnerability Assessment Subgroup (EVAS) is hereby established.

Objective:

To perform, or cause to be performed, assessments of the vulnerability of U.S. energy supplies and to identify and bring to the attention of the IG-EV recommendations to reduce the likelihood or impact of disruptions.

Purpose:

The purpose of the EVAS is to examine in advance of disruptions the vulnerability of U.S. energy systems to non-routine disruptions that may affect our national security and to propose options, which could be implemented in advance of disruptions, to increase the level of emergency preparedness.

Scope:

Energy systems to be examined are those which supply electric power, petroleum, natural gas, and coal within the United States. Analyses will consider both causes and effects of emergencies.

Procedure:

Selected and assigned analyses and evaluations will be conducted by the EVAS in accordance with guidance from the IG-EV. It shall be the policy of the EVAS to perform an integrating, rather than developmental, function where possible and to make maximum use of material developed in other forums and possibly for other purposes. In those instances when material necessary to support an analysis is clearly unavailable, the EVAS may undertake its development. Conclusions and recommendations of the EVAS will be presented to the IG-EV for its consideration.

Membership:

Membership of the EVAS shall be composed of representatives from the following departments and agencies:

Co-Chairmen:	Department of Defense Jeffrey A. Jones
	Department of Energy Robert M. Guth
Member Departments/ Agencies	Central Intelligence Agency Council of Economic Advisers Department of Agriculture Department of Commerce Department of Health and Human Services Department of Interior Department of Justice Department of State Department of Transportation Department of Treasury Federal Bureau of Investigation Federal Emergency Management Agency National Communications System National Security Council Nuclear Regulatory Commission Office of Management and Budget

Additional members may be added to the EVAS as required.

Appendix C

CHARTER OF THE DATABASE AND PROJECTIONS SUBGROUP OF THE INTERAGENCY GROUP ON ENERGY VULNERABILITY

Pursuant to National Security Decision Directive (NSDD) Number 188, "Government Coordination for National Security Emergency Preparedness," and by the direction of the Interagency Group on Energy Vulnerability (IG-EV), the Database and Projections Subgroup is hereby established.

Objective:

To provide an information base and analytical capabilities for the assessment of energy security issues.

Purpose:

The purpose of the Database and Projections Subgroup is to continue to develop an information base and forecasting methodologies for assessing the potential impacts of energy supply interruptions. The Subgroup will periodically assess the vulnerability of the United States to a disruption in oil supplies from the Middle East. This assessment will be expanded to cover other fuels, as appropriate.

Scope:

The Database and Projections Subgroup will develop baseline data and forecasts on the world oil market and assess U.S. vulnerability to a range of possible disruptions in oil supplies from the Middle East. This assessment will include: descriptions of the business-as-usual world oil situation and several hypothetical oil supply disruption cases; estimates of price and macroeconomic impacts of oil supply disruptions; and a discussion of the International Energy Agency's oil sharing agreement, the International Energy Program.

The Subgroup will develop a quarterly interagency consensus outlook for the international petroleum market. In addition, the Subgroup will develop and maintain appropriate methodologies for making near-term projections related to the business-as-usual petroleum market situation and the impacts of hypothetical petroleum supply disruptions.

The Subgroup will develop the above capabilities to serve two purposes: 1) to enable coordinated policymaking and market analysis related to energy emergency issues and 2) to maintain in a high state of readiness the operational capacity to assess the price and economic impacts of any actual supply disruption situations that may occur.

The Database and Projections Subgroup will expand this capability to address U.S. vulnerability related to electric power, natural gas, and coal as appropriate.

Procedure:

The Database and Projections Subgroup will conduct selected and assigned studies and evaluations under the guidance of the IG-EV. Recommendations by the Subgroup will be reviewed, approved, and coordinated by the IG-EV which will pass appropriate conclusions and recommendations to the Senior Interagency Group for National Security Emergency Preparedness (SIG-NSEP).

The Database and Projections Subgroup will continue to update the assessment of U.S. vulnerability to oil supply disruptions that has been prepared by its predecessor interagency working group since 1983. An Energy Evaluation (also known as the Blue Book) will continue to be issued twice a year and, as appropriate, may be expanded to include other fuels as provided in this Charter. During the interim quarters in which no updated report is issued, the Subgroup will develop a consensus outlook on the world oil situation for the business-as-usual case only. In addition, the Subgroup will, from time to time, develop information papers on specific aspects of energy vulnerability issues.

Members of the Subgroup will be invited to participate in, or send representatives to, quarterly Consensus Meetings to develop an interagency outlook focusing on the upcoming calendar quarter. The quarterly forecasts will be distributed to all Subgroup members for their use. Assumptions for the semi-annual update of An Energy Evaluation will be distributed to the Subgroup members for approval, as will the draft update of the analysis prepared on the basis of these assumptions and the consensus outlook.

Additional meetings of the Subgroup may be called by the chair on an as-needed basis.

The Subgroup will expand its capabilities beyond petroleum issues on the basis of recommendations by the Energy Vulnerability Assessment Subgroup and the Response Development Subgroup, as approved by the IG-EV.

Membership:

Membership on the Database and Projections Subgroup is open to all agencies that are members of the IG-EV and may include, as necessary, departments and agencies not designated as members of the IG-EV. Individuals designated as members of the Subgroup will be knowledgeable senior department or agency officials with appropriate security clearances and the authority to act on behalf of their department or agency. The following departments and agencies are members of the Subgroup:

Chaired by:	Department of Energy/Energy Information Administration
Member Departments/Agencies	Department of Commerce Department of Defense Department of the Interior Department of State Department of Transportation Department of the Treasury Central Intelligence Agency Council of Economic Advisers Federal Bureau of Investigation Federal Emergency Management Agency National Communications System National Security Council Office of Management and Budget

Additional members may be added as needed.

Appendix D

CHARTER OF THE
RESPONSE DEVELOPMENT SUBGROUP
OF THE
INTERAGENCY GROUP ON ENERGY VULNERABILITY

Pursuant to National Security Decision Directive (NSDD) Number 188, "Government Coordination for National Security Emergency Preparedness," and by direction of the Interagency Group on Energy Vulnerability (IG-EV) established by the Senior Interagency Group for National Security Emergency Preparedness (SIG-NSEP), the Response Development Subgroup (RDS) is hereby established.

Purpose:

The Response Development Subgroup will consider the implications of U.S. energy disruptions, and, as appropriate, develop proposed approaches for IG-EV review.

Objective:

The objective of the Response Development Subgroup is to enhance operational capability and develop proposed initiatives that could reduce susceptibility of U.S. energy systems to nonroutine disturbances, mitigate the impact of energy disruptions or threats to national security, or enhance capacity of energy systems to meet surge national security needs.

Scope:

The Response Development Subgroup wil review possible response options to reduce vulnerabilities of U.S. energy systems which include imports, production, refining, and distribuition of electric power, crude oil and petroleum products, natural gas, and coal.

Procedure:

The Response Development Subgroup work plan will be developed by the RDS co-chairmen in consultation with RDS members, subject to approval by the IG-EV. The co-chairmen will coordinate development of the RDS work plan with the other subgroup chairmen to ensure proper sequencing of efforts and to take into account other interagency analyses and efforts, such as the "High Level Review" of energy security. A primary focus of the RDS will be cooperation between industry and government to enhance energy security. The co-chairmen call RDS meetings, receive assignments from the IG-EV, transmit assignments to RDS members, brief the IG-EV on RDS progress, and assure timely completion of the RDS work plan.

Membership:

The Response Development Subgroup will be comprised of knowledgeable senior career officials with authority to act on behalf of their department or agency. RDS membership may include, as necessary, departments or agencies not designated as members of the IG-EV. Membership of the Response Development Subgroup includes:

Co-Chairs:
- Department of Energy (DOE)
- Department of State (State)

Members:
- Department of Defense (DOD)
- Department of the Interior (DOI)
- Department of Justice (DOJ)
- Department of Treasury (Treasury)
- Department of Transportation (DOT)
- Central Intelligence Agency (CIA)
- Council of Economic Advisers (CEA)
- Federal Bureau of Investigation (FBI)
- Federal Emergency Management Agency (FEMA)
- National Communications System (NCS)
- National Security Council (NSC)
- Nuclear Regulatory Commission (NRC)
- Office of Management and Budget (OMB)

LIST OF ACRONYMS

AST-6	Sixth Allocation Systems Test
CERM	Coordinated Emergency Response Measures
DIS	Disruption Impact Simulator
DOE	Department of Energy
DPS	Database and Projections Subgroup
EVAS	Energy Vulnerability Assessment Subgroup
IDAT	Interagency Damage Assessment Team
IEA	International Energy Agency
IG-EV	Interagency Group on Energy Vulnerability
NATO	North Atlantic Treaty Organization
NSDD	National Security Decision Directive
NSEP	National Security Emergency Preparedness
NSTAC	National Security Telecommunications Advisory Committee
NWOO	NATO Wartime Oil Organization
PPC	Petroleum Planning Committee
RDS	Response Development Subgroup
SIG-NSEP	Senior Interagency Group for National Security Emergency Preparedness
SPR	Strategic Petroleum Reserve